VPNBee manual

VPNBee is a firewall by Gayatri Hitech but it is more a product of products rather than a single product.

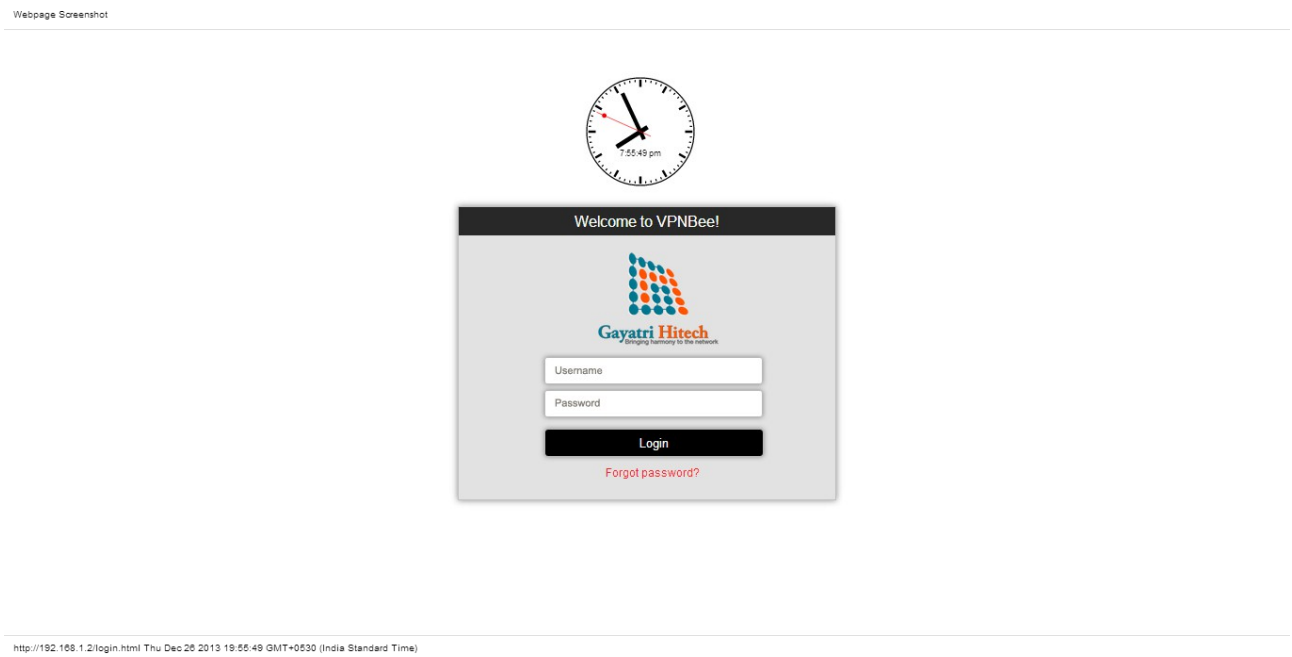
It is a VPN server and client, you can do captive portal with it, you have IP filtering and QoS rules, you have server load balancing, ISP link concentration, site to site failover, web caching, proxying, URL filtering and much more.

The help for this product as in our other products is made available online using the swimming ring logo for page level help and the info logo for panel level help.

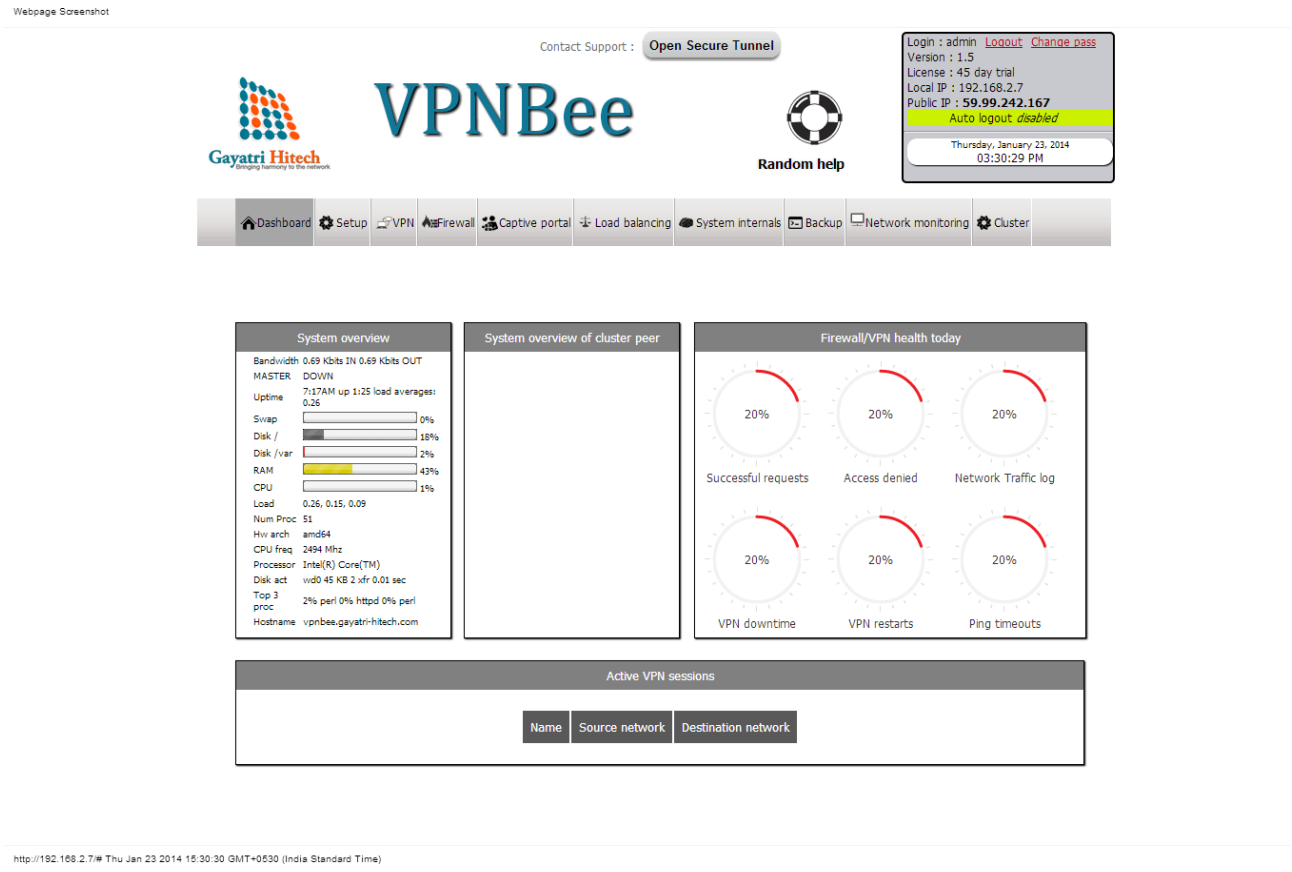
This help document is deliberately kep terse and to the point to avoid information overload.

Should you have any questions you are welcome to send us an e-mail or contact us by phone or chat for clarifications.

After you configure the IP address, network mask and gateway using nCurses interface you can start using the web interface of the product using HTTP or HTTPS which throws up a login screen like this.



After you login you are shown a dashboard screen like below.



Then you can click at **Setup -> Installation**. You can change the IP address of VPNBee or change the network mask or gateway here. You can also add IP alias addresses and set the hostname and local network range here.

Contact Support : Open Secure Tunnel

Gayatri Hitech

VPNBee

Random help

Login : admin Logout Change pass
Version : 1.5
License : 45 day trial
Local IP : 192.168.2.7
Public IP : **59.99.242.167**
Auto logout *disabled*
Thursday, January 23, 2014
11:31:52 AM

Install and configure VPNBee

Network configuration

Network interface	em0
Link status	UP
IP address	192.168.2.7
Subnet mask	255.255.255.0

Save

Default gateway

gateway [ ] save

Our local network

Our network in CIDR 10.0.0.0/8 Save

Static routes

Select	Destination	Gateway
☐	2.3.4.50	192.168.1.1
☐	2.3.4.0/8	2.3.38.4

Delete

Add new static route

Destination [ ]
Gateway [ ]
Add

Existing alias Addresses

Select	Interface	IP address	Netmask
☐	em0	3.3.4.80	255.0.0.0
☐	em0	2.3.4.4	255.255.255.0
☐	fxp0	2.3.40.3	255.255.0.0

Delete

Found 3 alias addresses

Add new IP alias

Alias IP address [ ]
Alias Network Mask [ ]
Network Interface em0 UP
Save

Our Hostname

Our hostname/FQDN lathae.gayatri-hitech.com Save

Dynamic IP updates using NO-IP protocol

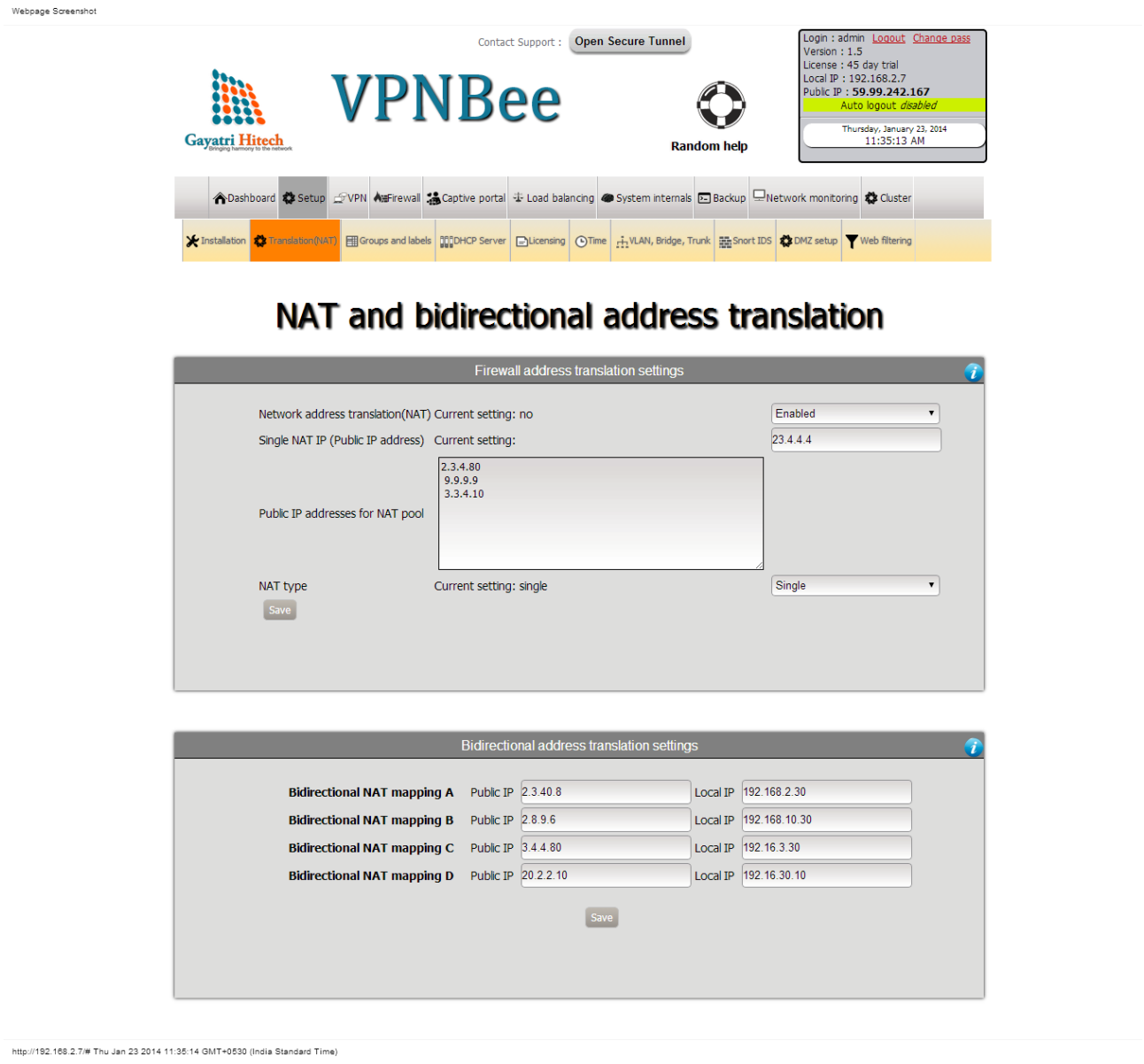
Dynamic DNS	Current setting:	YES
Our DNS name(FQDN)	stream.in	
Key for updating IP address	footer	

Save

You can also configure dynamic DNS update using the no-ip protocol. Dynamic DNS updates are useful for setting up VPN nodes without a static IPv4 address.

VPNBee comes with very sophisticated NAT features configured using the **Address translation** menu. You can also configure public IP to local IP mapping which can be more effective and convenient than traditional port forwarding of certain ports to certain local IP addresses.

The NAT public IP addresses can be assigned to local hosts accessing the Internet one after another using different algorithms like hash, round robin, random etc.

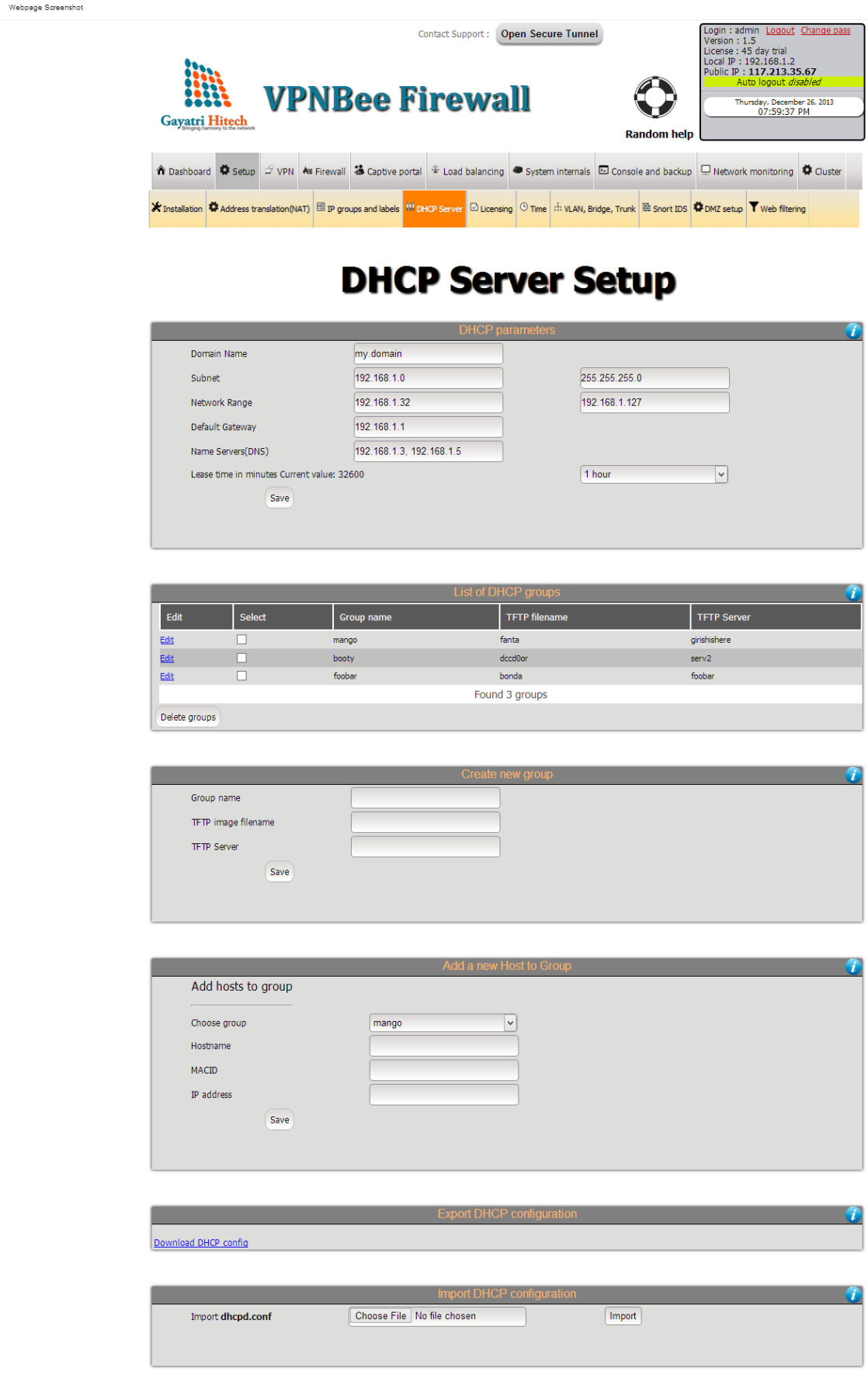


You can then configure host names to local IP addresses and group hosts into 5 predefined groups for easier network maintenance. These groups are used

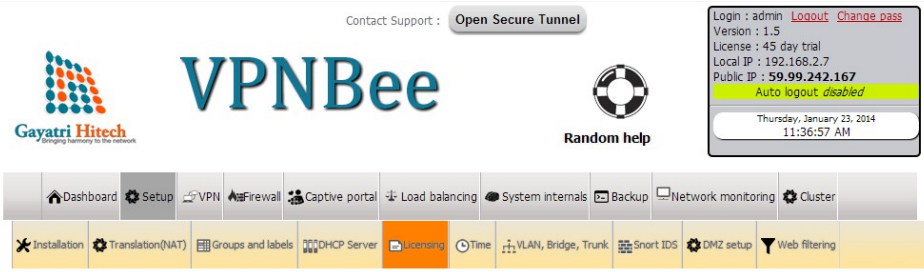
throughout VPNBee for setting rules to the entire group instead of to hosts one by one. The menu is **labels and groups**.

VPNBee gives a very easy drag and drop interface for configuring groups.

Following this action you may wish to setup **DHCP server** which is a fairly feature rich and comprehensive component in VPNBee using which you can serve TFTP files to thin clients and setup DHCP groups and do much more.



You then have the **Licensing** menu. You will be loading the license file into VPNBee using this menu.



License information

Load license

Upload New license Choose File No file chosen Upload license

License information

Description	
License ID	
Type	
Number of Users	
Status	You have -40 days to go
Organization	
Address	
Contact Person name	
Contact e-mail	
Telephone	
Mobile	
Fax	

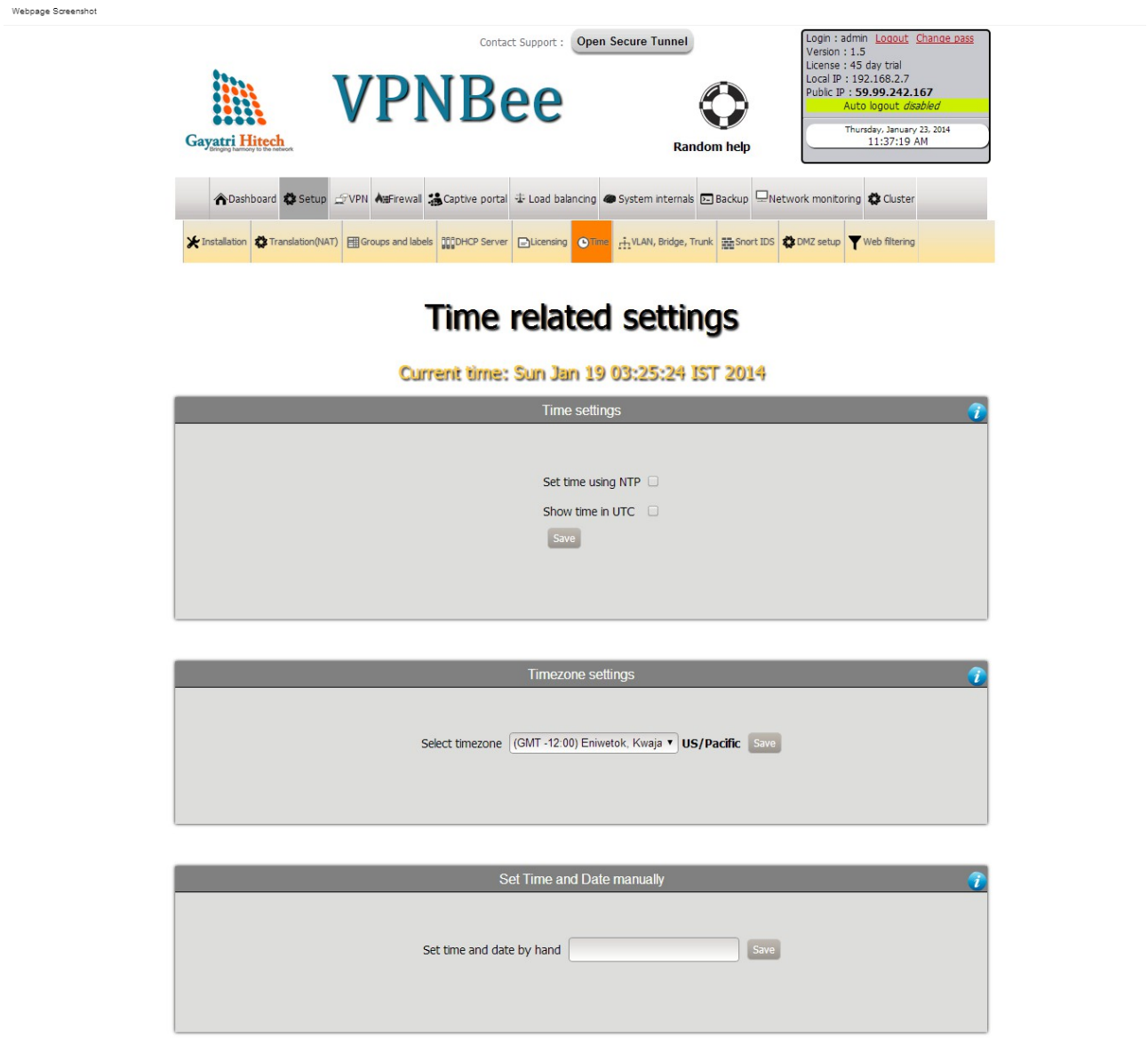
License validity

Issued date	Mon Dec 9 03:55:39 IST 2013
Expiry date	Mon Dec 9 03:55:39 IST 2013

License usage

Description	
Max daily usage	
Avg daily usage	

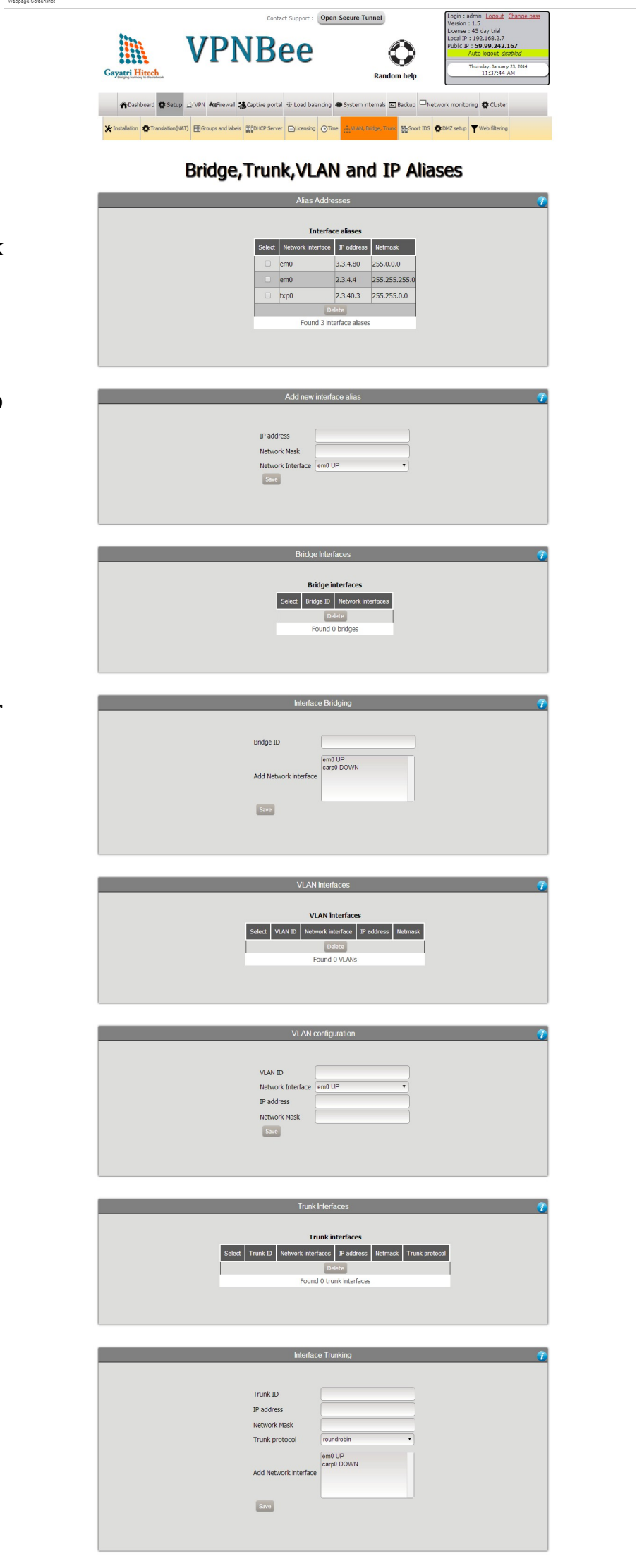
Then you have the **Time** menu using which you can configure the time as well as the timezone of your geographical location.



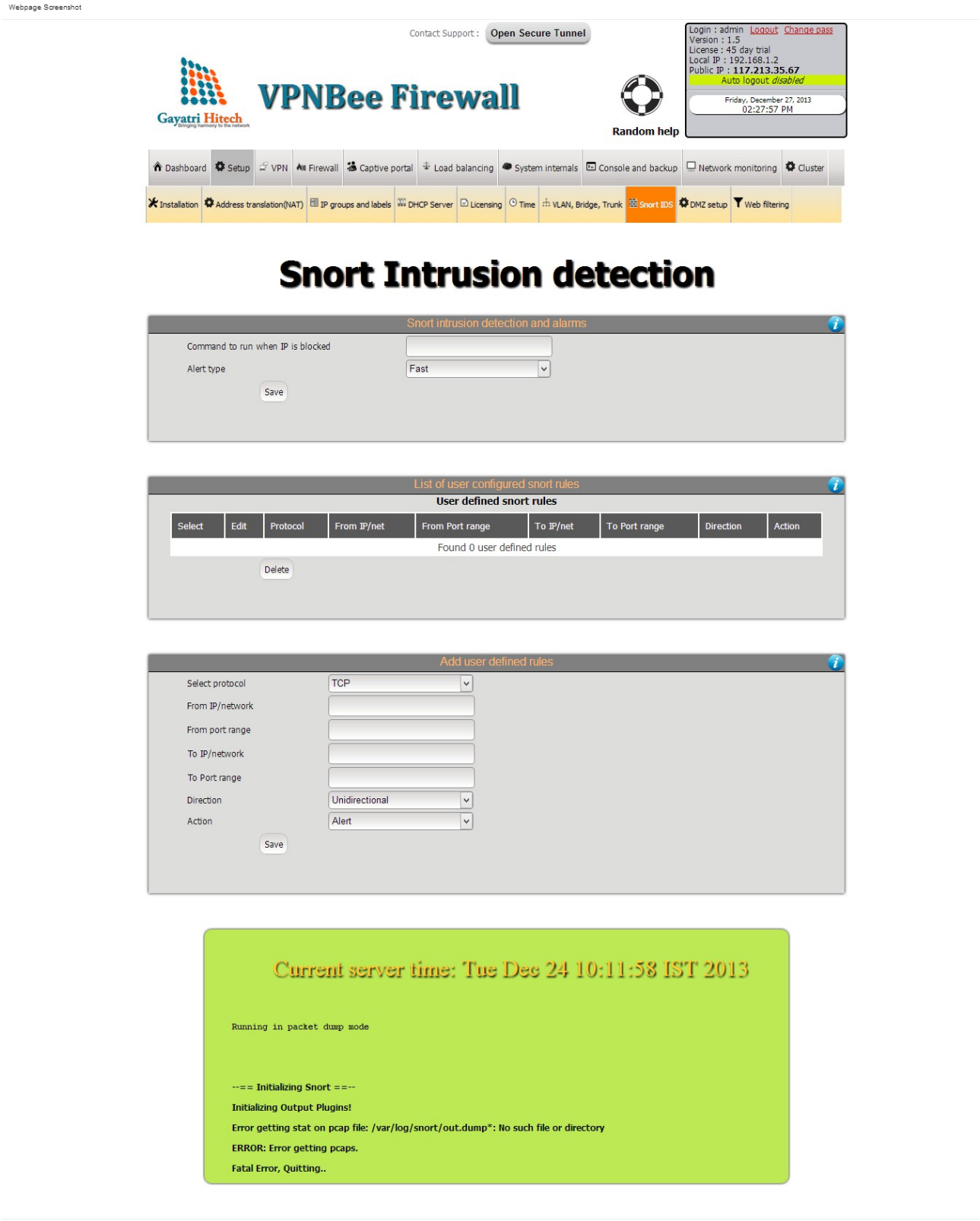
Then you have the **VLAN,Bridge,Trunk** menu which helps you setup VLAN interfaces , bridge together multiple physical interfaces and create the special trunk interface which can be very useful for doing sophisticated network level failover and load balancing with multiple physical links.

Note that this menu item is for advanced purposes and not meant for novices in networking.

You can then invoke the network sniffer in **Snort IDS** menu. Alternately you can also configure alerts on matching packet signatures. Snort has become a very powerful and popular network level intrusion detection tool which can be inevitable in the face of any new DdoS attacks or



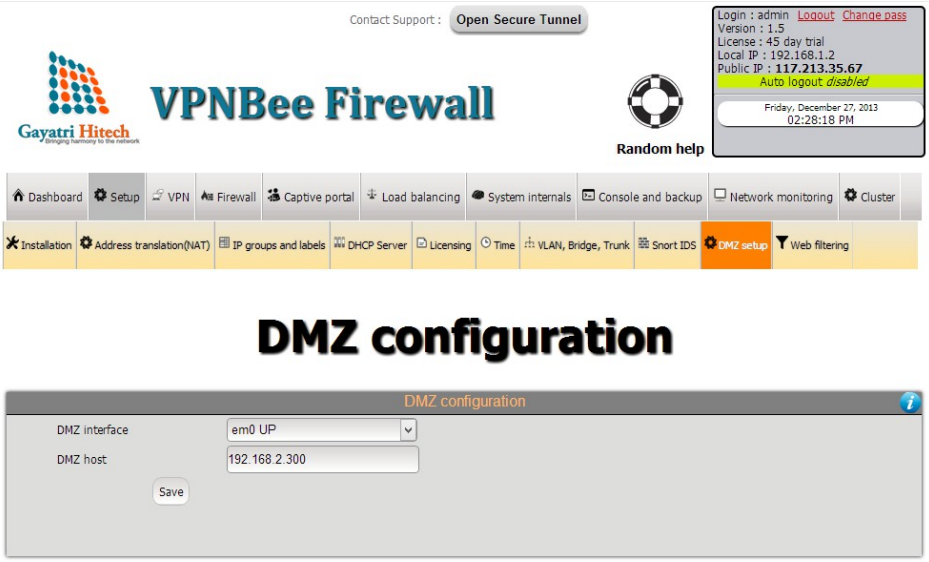
compromises or some new virus or worm affecting Windows machines or some commercial vendors.



Anyone who has used a firewall knows what is meant by DMZ or de militarized zone. These are hosts which run public applications and thereby are connected with the outside world(big bad Internet) and they do not have communication

with the local network. This is done in order to prevent compromises from affecting our precious local network.

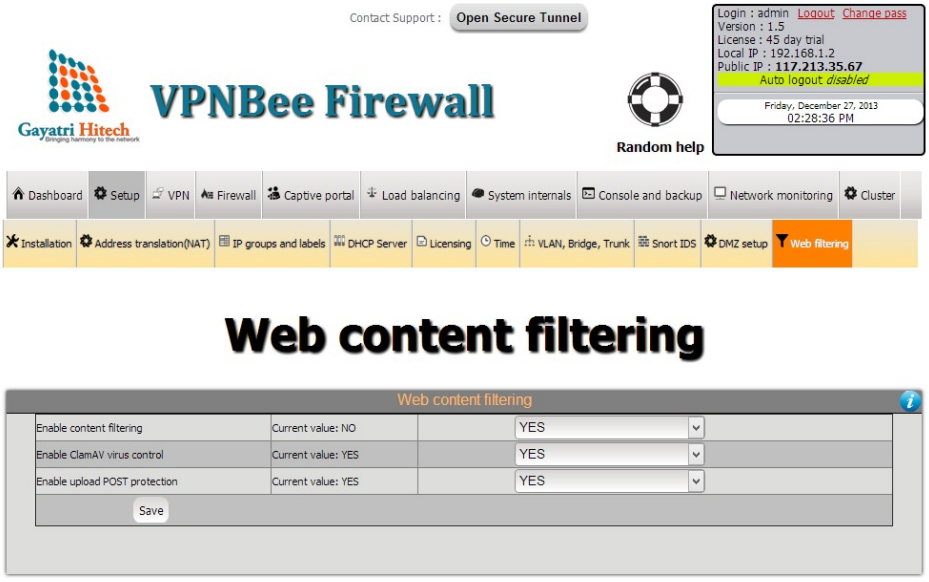
Webpage Screenshot



http://192.168.1.2/index.html Fri Dec 27 2013 14:28:19 GMT+0530 (India Standard Time)

Then you have the **Web filtering** menu**.** Using this you can perform dansguardian category based web browsing, child content monitoring and much more.

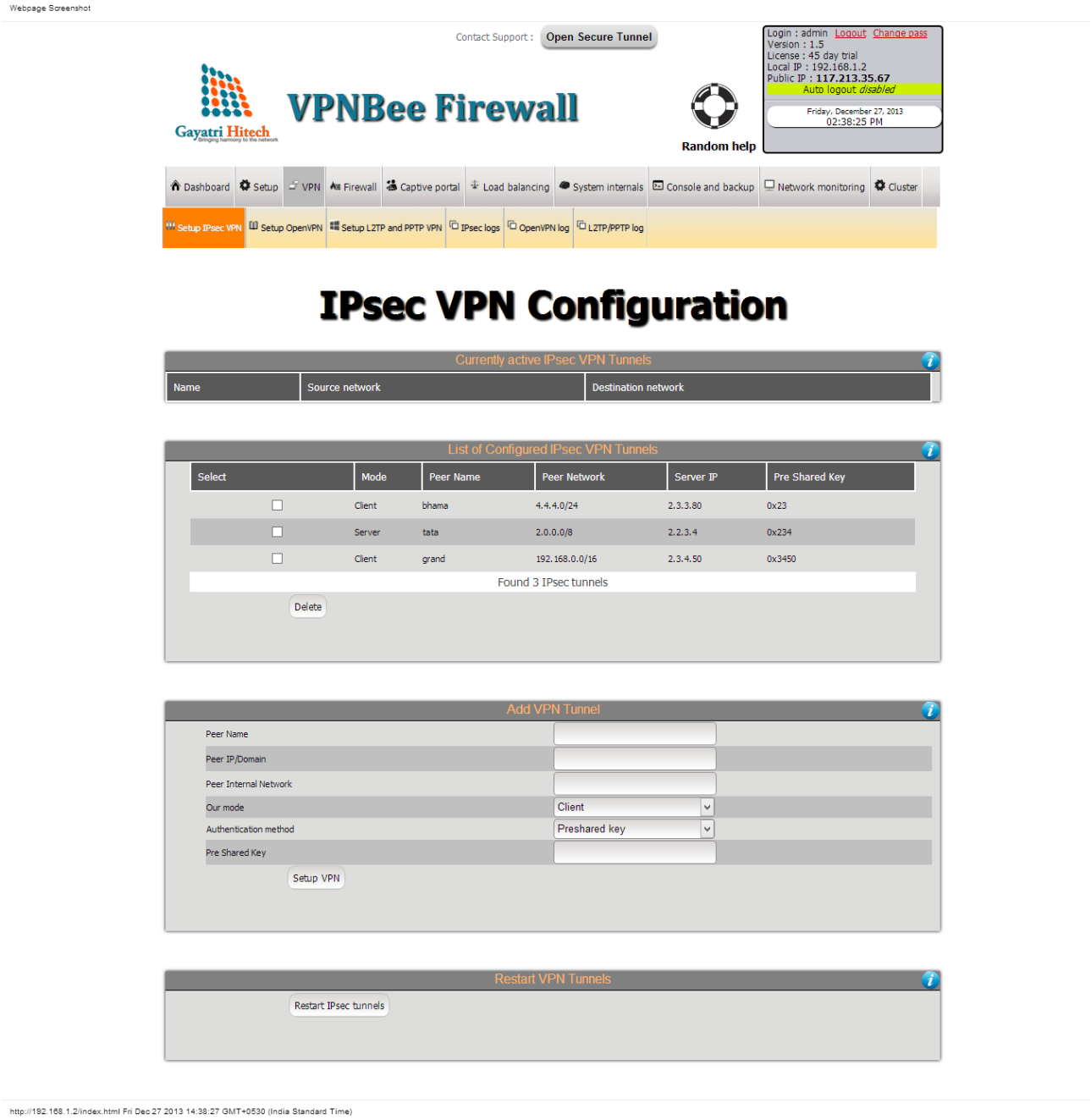
Webpage Screenshot



http://192.168.1.2/index.html Fri Dec 27 2013 14:28:37 GMT+0530 (India Standard Time)

Then you can look at the **VPN -> Setup Ipsec VPN** menu. VPNBee highly recommends using IPSec VPN when you have choice of setting up VPN between two nodes. VPNBee Ipsec VPNs are well tested, very stable and have very little payload overhead and CPU load.

You can easily constructed a partial mesh with multiple VPNBee nodes and using pre shared keys.

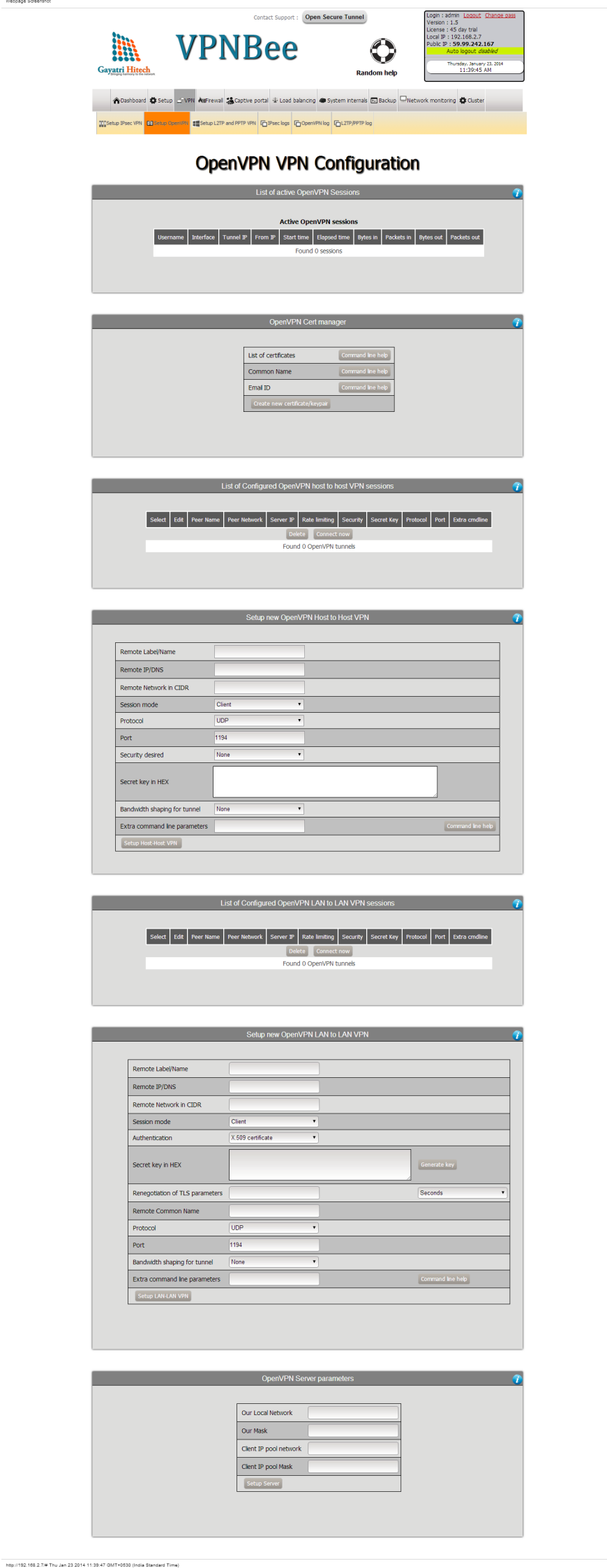


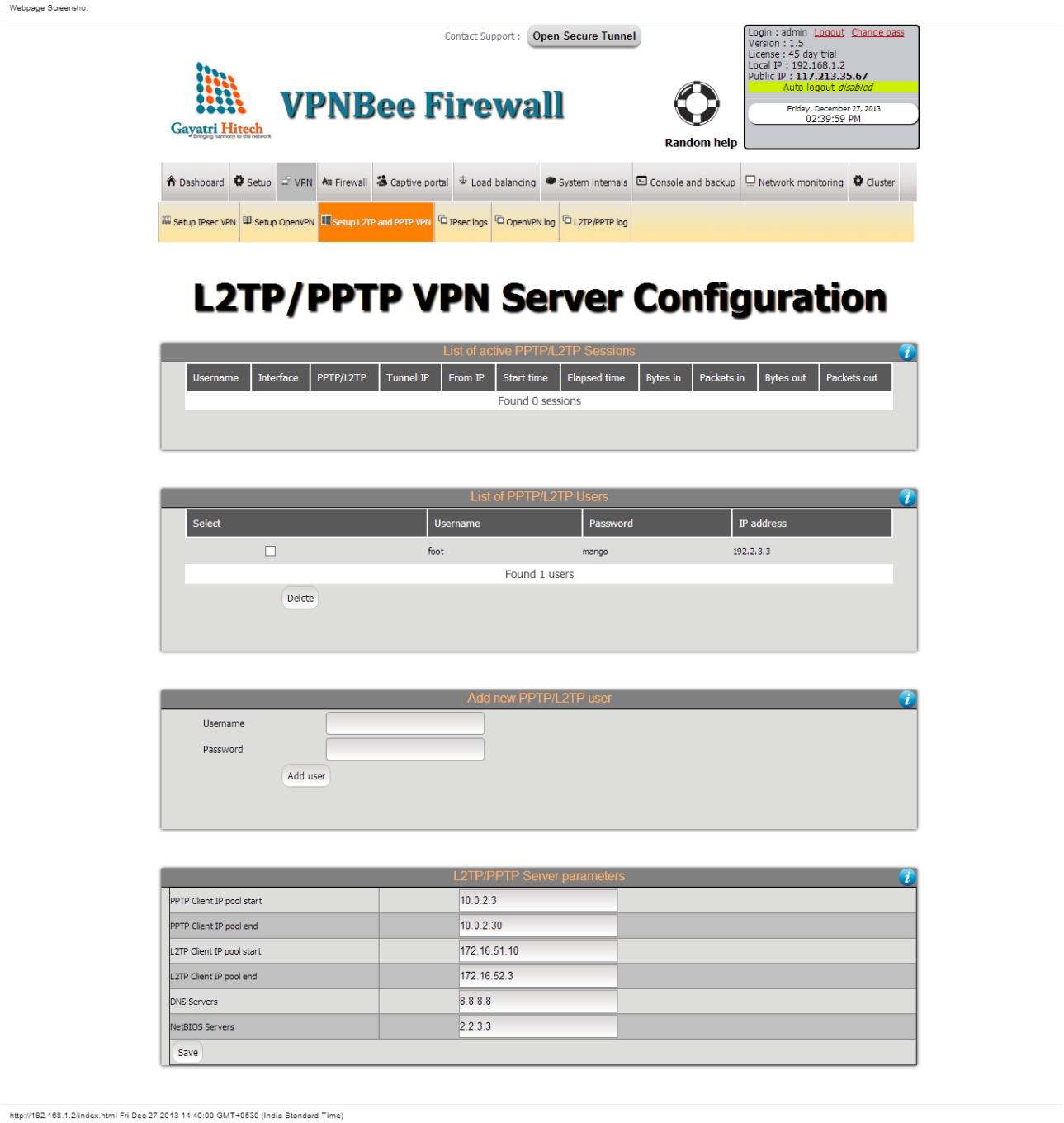
You can also inspect the currently active sessions and restart all tunnels using this interface. The ability to restart VPN tunnels individually will be added in future releases of VPNBee.

You then have the **Setup OpenVPN** menu using which you can create OpenVPN certificates, do sophisticated OpenVPN tunnel setup and inspect the existing tunnels and view the packets and bytes transferred etc.

You also have the ability to setup L2TP or PPTP VPN tunnels using the **Setup L2TP and PPTP VPN** menu. You can easily connect to Windows machines without installing any software application using L2TP or PPTP by creating Windows usernames and passwords in VPNBee.

It is also trivial to view the statistics of packets and bytes sent and received using the live sessions view in VPNBee.

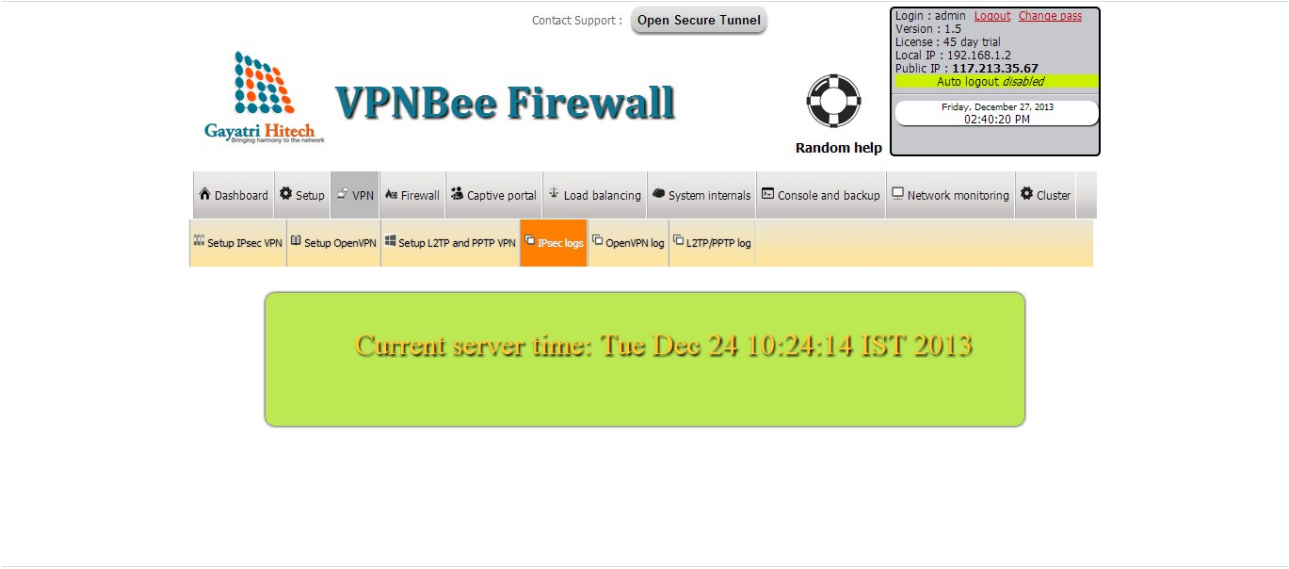




Note that the usernames and passwords are shared between PPTP and L2TP.

You can view the logs of these 3 VPN technologies using the screens as seen below.

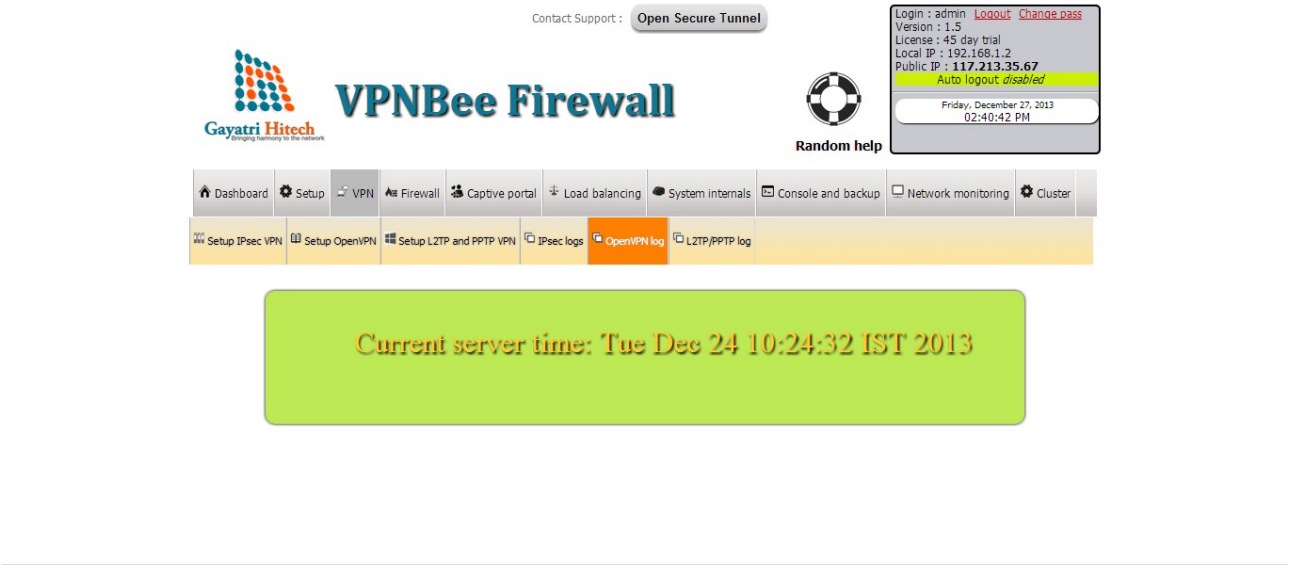
Webpage Screenshot



http://192.168.1.2/index.html Fri Dec 27 2013 14:40:21 GMT+0530 (India Standard Time)

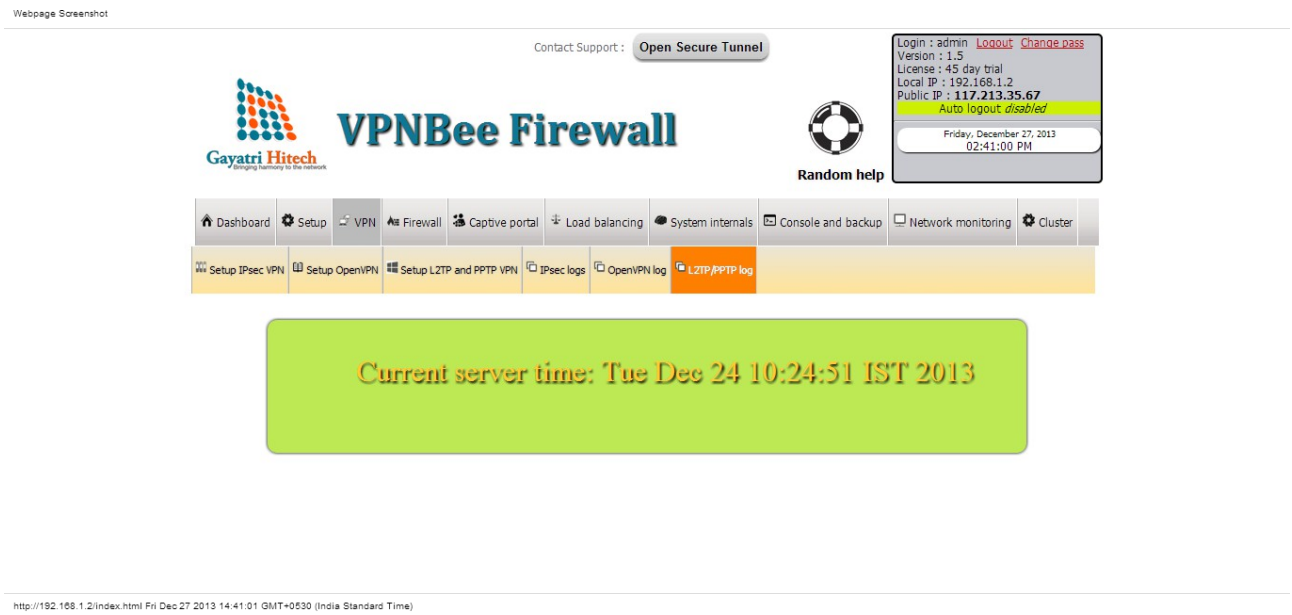
This is the **OpenVPN Logs** menu.

Webpage Screenshot



http://192.168.1.2/index.html Fri Dec 27 2013 14:40:43 GMT+0530 (India Standard Time)

Finally the **L2TP/PPTP logs.**



Then we move on to the **Firewall -> Group Settings** menu item.

You can configure the allowed protocols, bandwidths allocated to each predefined group here using easy configuration widgets.

Contact Support : Open Secure Tunnel

Gayatri Hitech

VPNBee Firewall

Random help

Login : admin Logout Change pass
Version : 1.5
License : 45 day trial
Local IP : 192.168.1.2
Public IP : 117.213.35.67
Auto logout disabled
Friday, December 27, 2013
03:03:23 PM

Firewall groups setup

Local group rule settings

Fullaccess group allowed TCP protocols

Available: HTTP, SMTP, RSYNC, FTP, SSH, DNS
Selected:

Sort / Top / Up / Down / Bottom

Fullaccess group allowed UDP protocols

Available: DNS
Selected: NTP, SNMP

Sort / Top / Up / Down / Bottom

Restricted access group allowed TCP protocols

Available: HTTP, SMTP, RSYNC, FTP, SSH, DNS
Selected:

Sort / Top / Up / Down / Bottom

Restricted access group allowed UDP protocols

Available: NTP, DNS
Selected: SNMP

Sort / Top / Up / Down / Bottom

Custom1 group allowed TCP protocols

Available:
Selected: HTTP, SMTP, RSYNC, FTP, SSH, DNS

Sort / Top / Up / Down / Bottom

Custom1 group allowed UDP protocols

Available: NTP, DNS
Selected: SNMP

Sort / Top / Up / Down / Bottom

Custom2 access group allowed TCP protocols

Available: SMTP, RSYNC, FTP, SSH
Selected: HTTP, DNS

Sort / Top / Up / Down / Bottom

Custom2 group allowed UDP protocols

Available: NTP, SNMP, DNS
Selected:

Sort / Top / Up / Down / Bottom

Custom3 group allowed TCP protocols

Available: RSYNC, FTP, SSH
Selected: HTTP, SMTP, DNS

Sort / Top / Up / Down / Bottom

Custom3 group allowed UDP protocols

Available: NTP, DNS
Selected: SNMP

Sort / Top / Up / Down / Bottom

Save

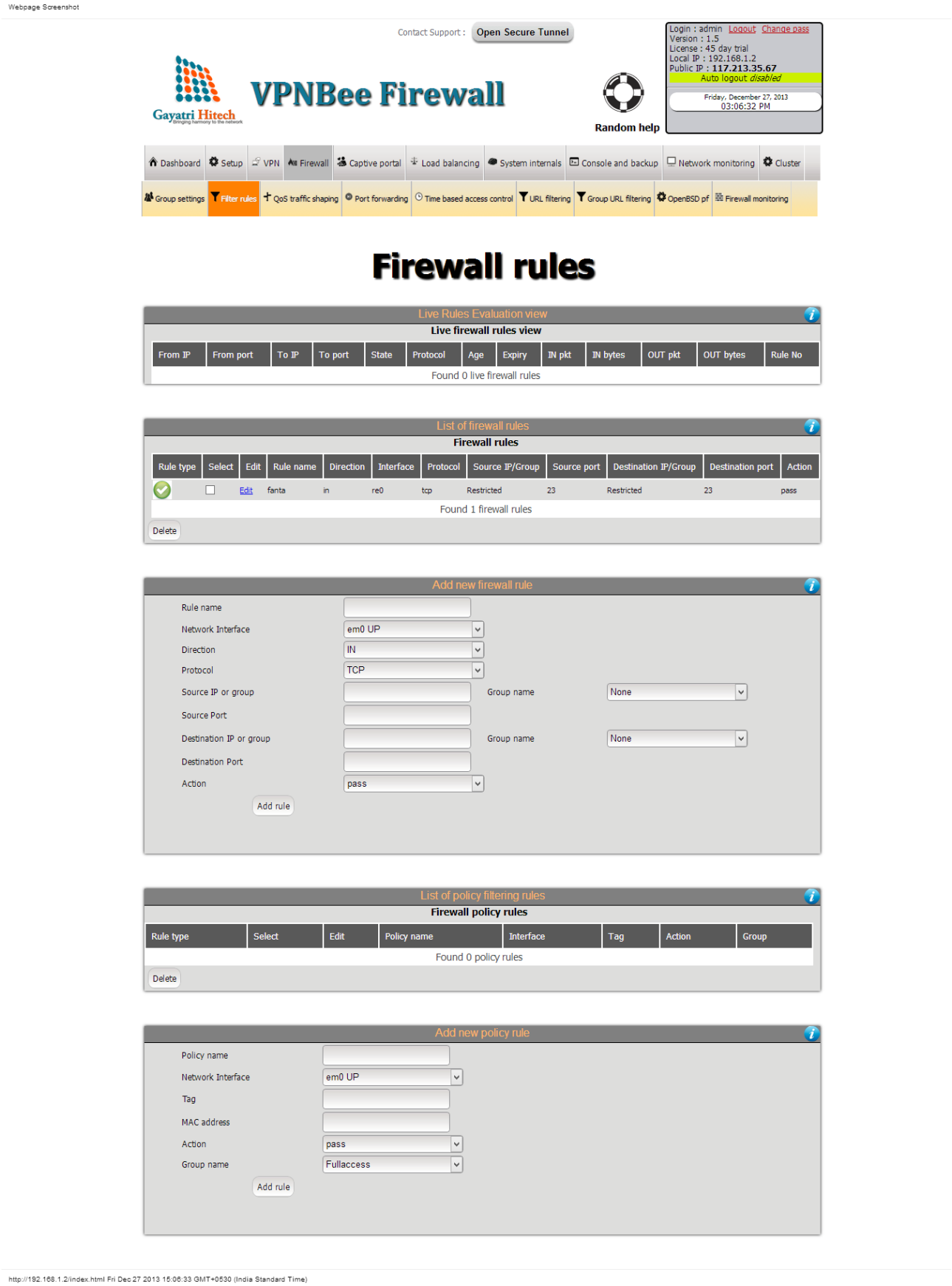
Local group bandwidth settings

Full access group bandwidth	Current setting: 1mbps	1 MBPS
Restricted group bandwidth	Current setting: 1mbps	1 MBPS
Custom1 group bandwidth	Current setting: 1mbps	1 MBPS
Custom2 group bandwidth	Current setting: 1mbps	1 MBPS
Custom3 group bandwidth	Current setting: 1mbps	1 MBPS

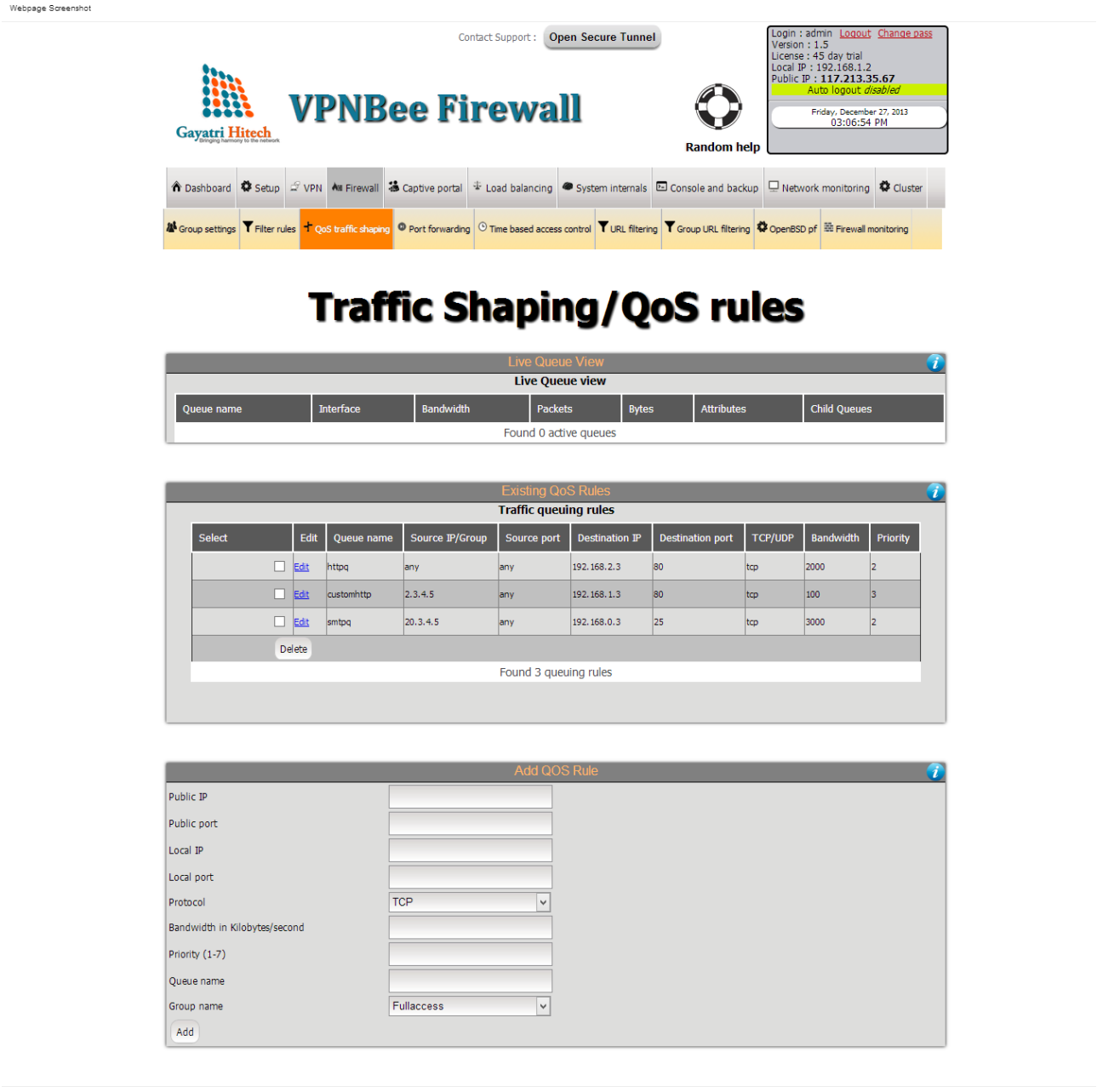
Save

Then you have the **Filter rules** menu using which we can configure various port and IP blocking rules. You can create rules for individual hosts as well as define rules for host groups defined elsewhere.

Using filter rules you can easily control which hosts gain access to which protocols on the Internet. This is the most basic setup a network administrator does to protect your network from abuse by insiders.



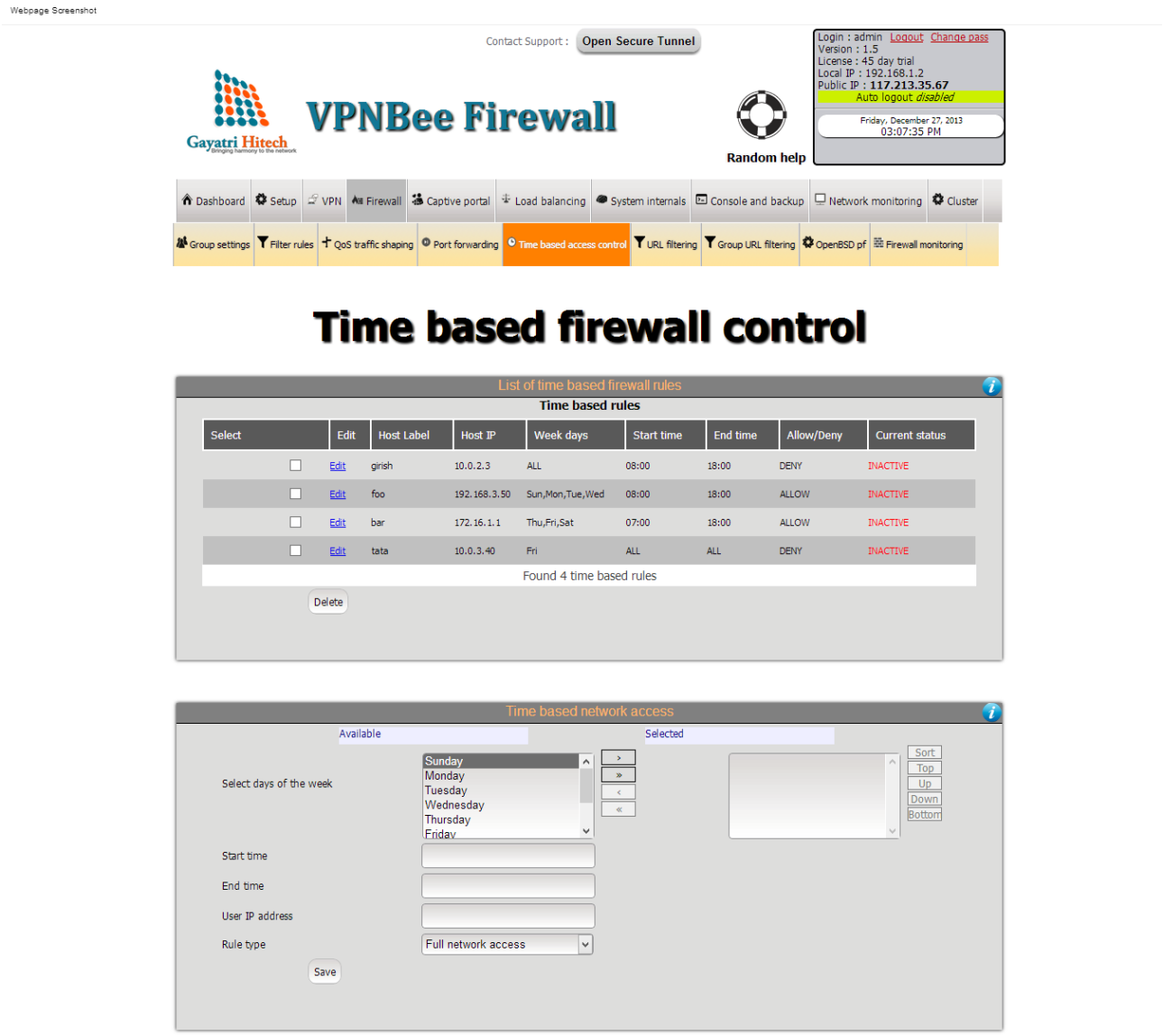
Then you have the **QoS traffic shaping** menu. We can perform packet queueing to rate limit the traffic leaving VPNBee using this menu. We can apply rules to individual hosts running protocols or even to groups.



You can also view the bandwidth allocated to each queue using the live queue view.

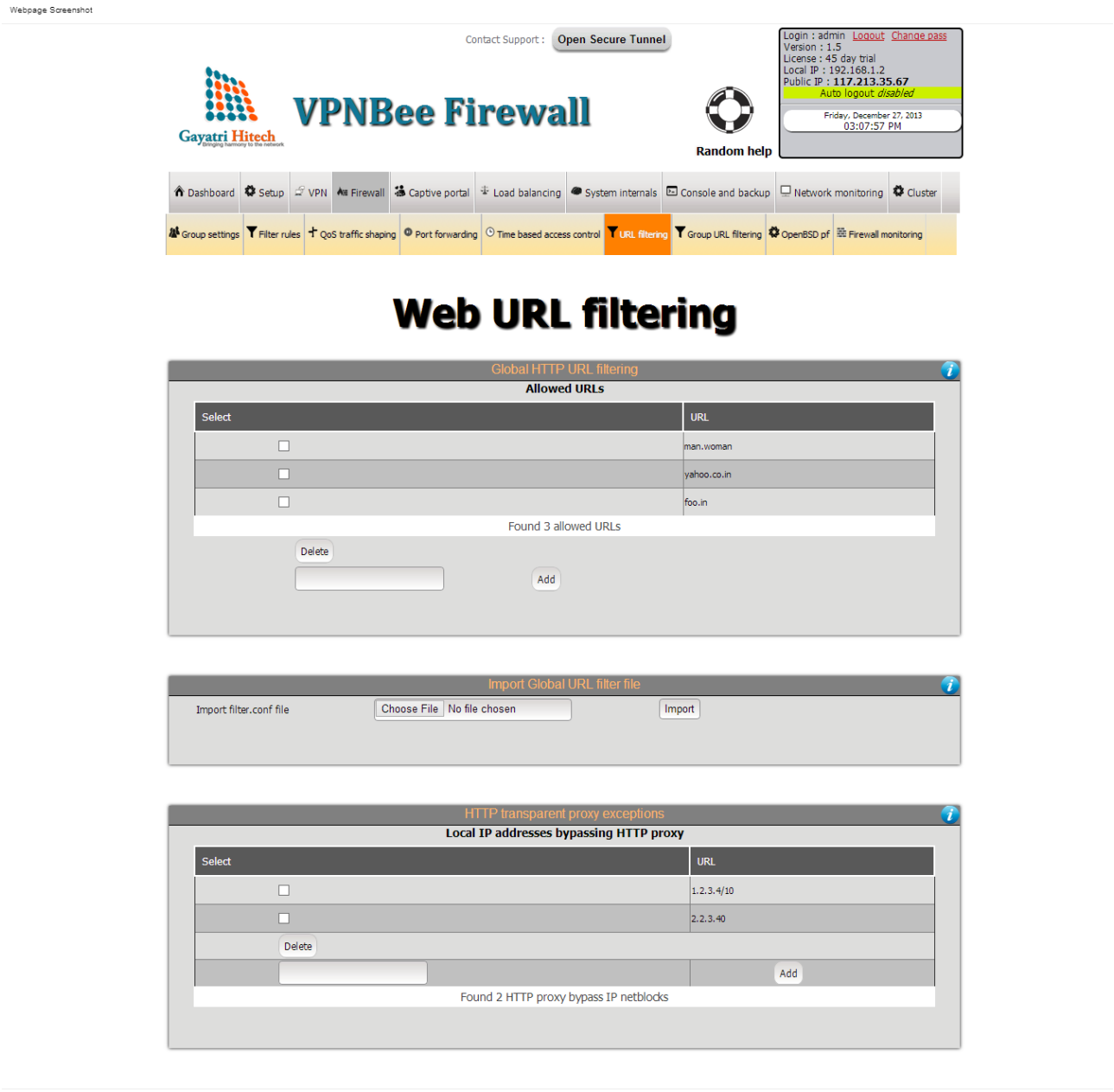
Then you can perform port forwarding to redirect traffic showing up on public ports to local IP addresses and local ports using the **Port forwarding** menu.

Then you have to click at **Time based access control**. Using this you can allow or deny Internet access based on time of the day and day of the week.

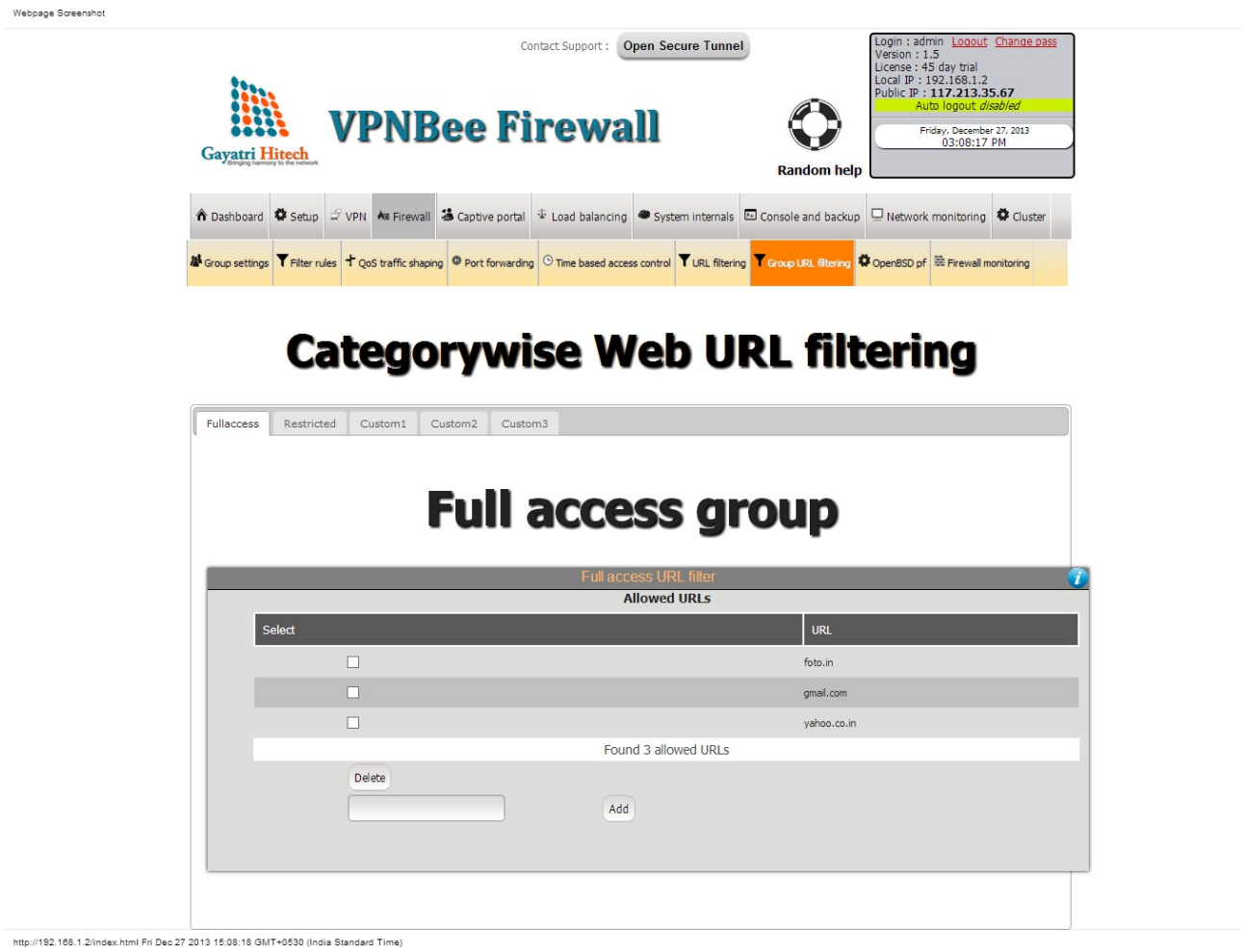


You can look at the **URL filtering** menu. The URLs that are allowed by VPNBee are listed here. You can also optionally perform group URL filtering in the next menu.

You can configure the list of allowed URLs one by one or import the list with a file upload.



The next screen **Group URL filtering** does the same as URL filtering in which each group of hosts as defined elsewhere gets to access the URLs as listed in this menu.



Then you can click at **OpenBSD pf** for configuring certain advanced rule parameters. Note that this feature is a very advanced use and any mistake here can cause unintended consequences if you do not have experience with OpenBSD pf.

Contact Support : Open Secure Tunnel

Gayatri Hitech

VPNBee Firewall

Random help

Login : admin Logout Change pass
Version : 1.5
License : 45 day trial
Local IP : 192.168.1.2
Public IP : 117.213.35.67
Auto logout :disabled
Friday, December 27, 2013
03:08:36 PM

Dashboard | Setup | VPN | Firewall | Captive portal | Load balancing | System internals | Console and backup | Network monitoring | Cluster

Group settings | Filter rules | QoS traffic shaping | Port forwarding | Time based access control | URL filtering | Group URL filtering | OpenBSD pf | Firewall monitoring

OpenBSD pf settings

Rule specific settings

Configured rule options

Rule options

Select	Edit	Rule name	Type of Service	Label	TCP flags	Probability	Tag

Found 0 configured options

Delete

Extra options to rules

TOS

Label: Source IP

TCP flags

FIN bit
SYN bit
ACK bit
RSET bit
PUSH bit
URG bit
ECE bit
CWR bit

Probability(in %)

Tag: Source IP

Set for group: Fullaccess

Save

Configured TCP state tracking options

TCP state tracking options

Select	Edit	Rule name	Option type	Source tracking	Conn type	Timeout	Max states	Max src nodes	Max src states	Max src conn	Max src conn rate

Found 0 state tracking rules

Delete

TCP state parameters

Floating/ifbound — Current setting : — Floating

Source tracking — Current setting : — Global

Max states

Timeout: 10

Maximum source nodes

Maximum source states

Maximum source connections

Maximum source connection rate

TCP connection type — Current setting : — Synproxy state

Set for TCP rule: fanta in re0 Restricted 23 Res

Save

Configured Address pool rules

Address pool rules

Select	Edit	Rule name	Address selection algorithm	Forwarding method
	Edit	latha is here now		

Found 1 state tracking rules

Delete

Address pool parameters

Address selection algorithm: Hash

Type of routing: route-to

Set for rule: fanta in re0 Restricted 23 Res

Save

Global firewall settings

State expiry/timeout settings

TCP Closed	20
TCP Closing	30
TCP Established	40
TCP Finwait	60
TCP First	80
TCP Opening	90
ICMP error	30
ICMP First	30
UDP first	20
UDP multiple	10
UDP single	80
Other first	20
Other multiple	40
Other single	30

Save

Traffic normalization/scrub settings

Maximum MSS: 20

Minimum TTL: 30

NO DF

Random ID

Reassemble TCP

Save

State Options settings

Optimization — Current setting : aggressive — Aggressive

Reassemble fragments

State policy — Current setting : — Interface bound

Blocking packets policy — Current setting : — Drop

Limit states: 2000

Limit fragments: 5000

Save

You then have **Firewall monitoring** which can give you enough detail about how your various rules configured in the top level menu **Firewall** are working.

But to make sense out of the output you will have to gain some experience with these numbers.

PF firewall states and timers

PF firewall high level parameters

Status	
Duration	
Total bytes in	
Total bytes out	
IN pkts passed	
IN pkts blocked	
OUT pkts passed	
OUT pkts blocked	
Total states	0
Total state searches	0
Total state inserts	0
Total state removals	0
Total state matches	0
Bad offsets	0
Fragments	0
Short packets	0
Bad timestamps	0
Congestion	0
Packets with IP options	0
Packets with cksum mismatch	0
Maximum states per rule	0
Maximum states per source IP	0
Maximum source IP nodes	0
Maximum source IP connections	0
Maximum source IP connection rate	0

PF firewall timers

tcp.first	120s
tcp.opening	30s
tcp.established	86400s
tcp.closing	900s
tcp.finwait	45s
tcp.closed	90s
tcp.tsdiff	30s
udp.first	60s
udp.single	30s
udp.multiple	60s
icmp.first	20s
icmp.error	10s
other.first	60s
other.single	30s
other.multiple	60s
frag	60s
interval	10s
adaptive.start	6000
adaptive.end	12000
src.track	0s

PF firewall limits

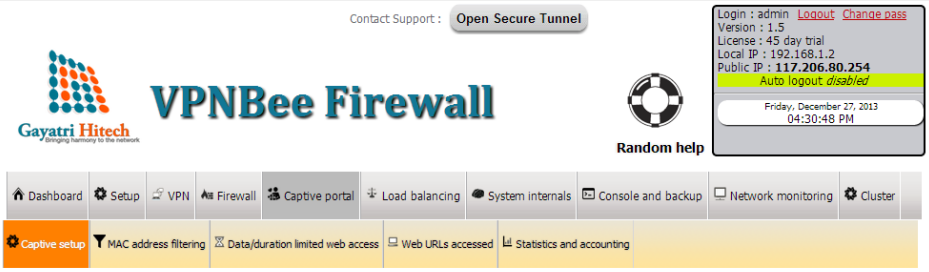
states	10000
src-nodes	10000
frags	1536
tables	1000
table-entries	200000

PF protocol states

From IP	From port	To IP	To port	State	Protocol	Age	Expiry	IN pkt	IN bytes	OUT pkt	OUT bytes	Rule No

You then have the captive portal implementation which is useful for Wifi hotspots in hotels and coffee shops.

Please click at **Captive portal -> Captive setup**. Using this menu you can define the legalese you wish to show to users as well as configure the TCP ports, URLs, IP addresses and MAC addresses that you wish to whitelist to bypass the captive portal software.



Captive portal setup

Captive portal access page

Disclaimer/legalese

```
                obtain updates.
  for more details
 please go to
  http://www.maxmind.com/app/products

  see https://www.maxmind.com/app/license_key_login to obtain
License Key

  UserId
 and available ProductIds
```

Save

List of captive users

User based access rules

Select	Edit	Username	Password	Payment type
☐	Edit	dread	bash	Postpaid
☐	Edit	girish	panache	Prepaid

Found 2 captive users

Delete

Add captive users

Username

Password

Payment type: Prepaid

Save

List of whitelist entries

User based access rules

Select	Whitelist entry name	TCP port	MAC address	HTTP URL	IP address
☐	soon			www.yahoo.com	
☐	someport		2346		

Found 2 whitelist entries

Delete

Add whitelist entries

Entry label

MAC address

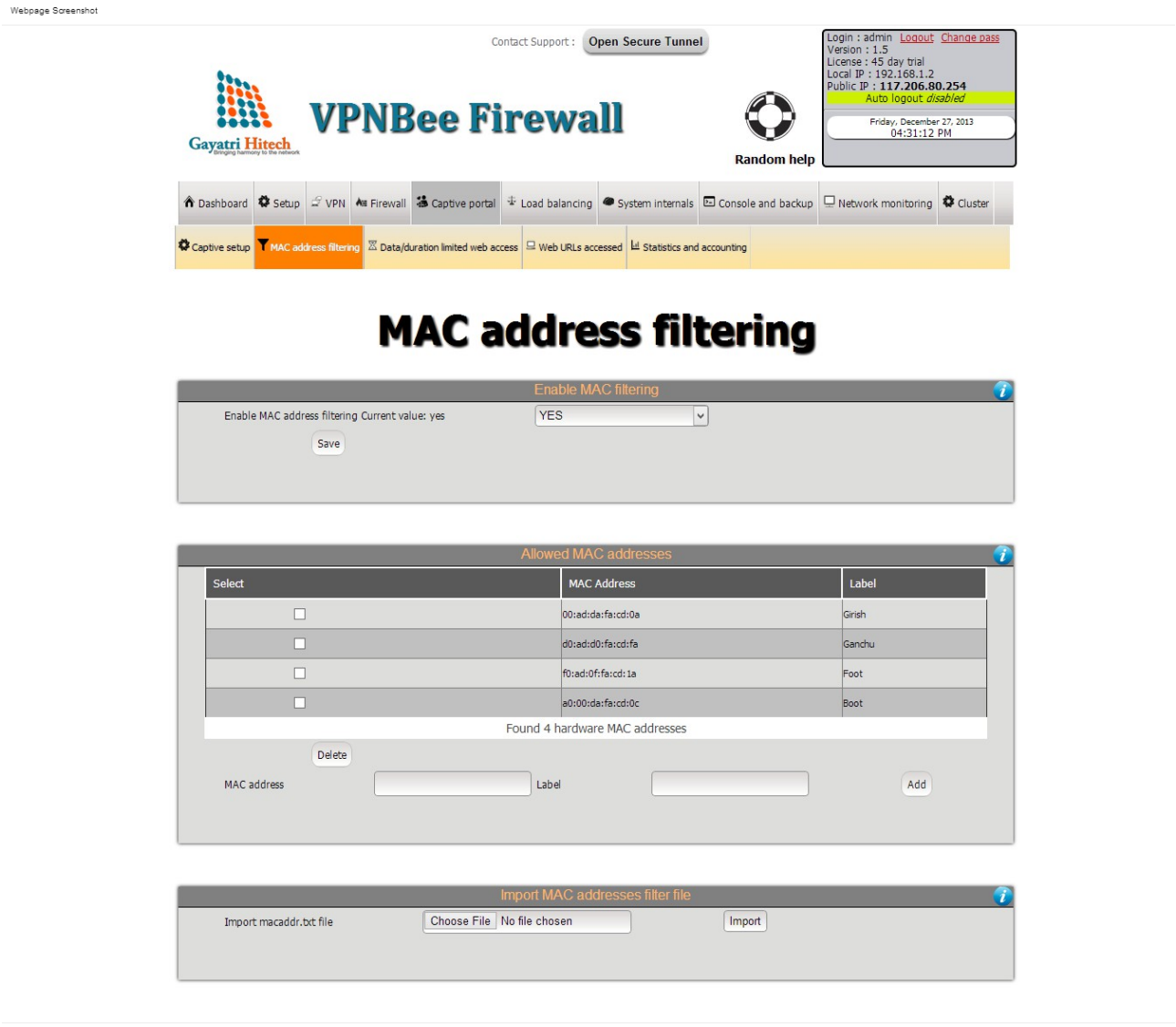
TCP port

HTTP URL

IP address

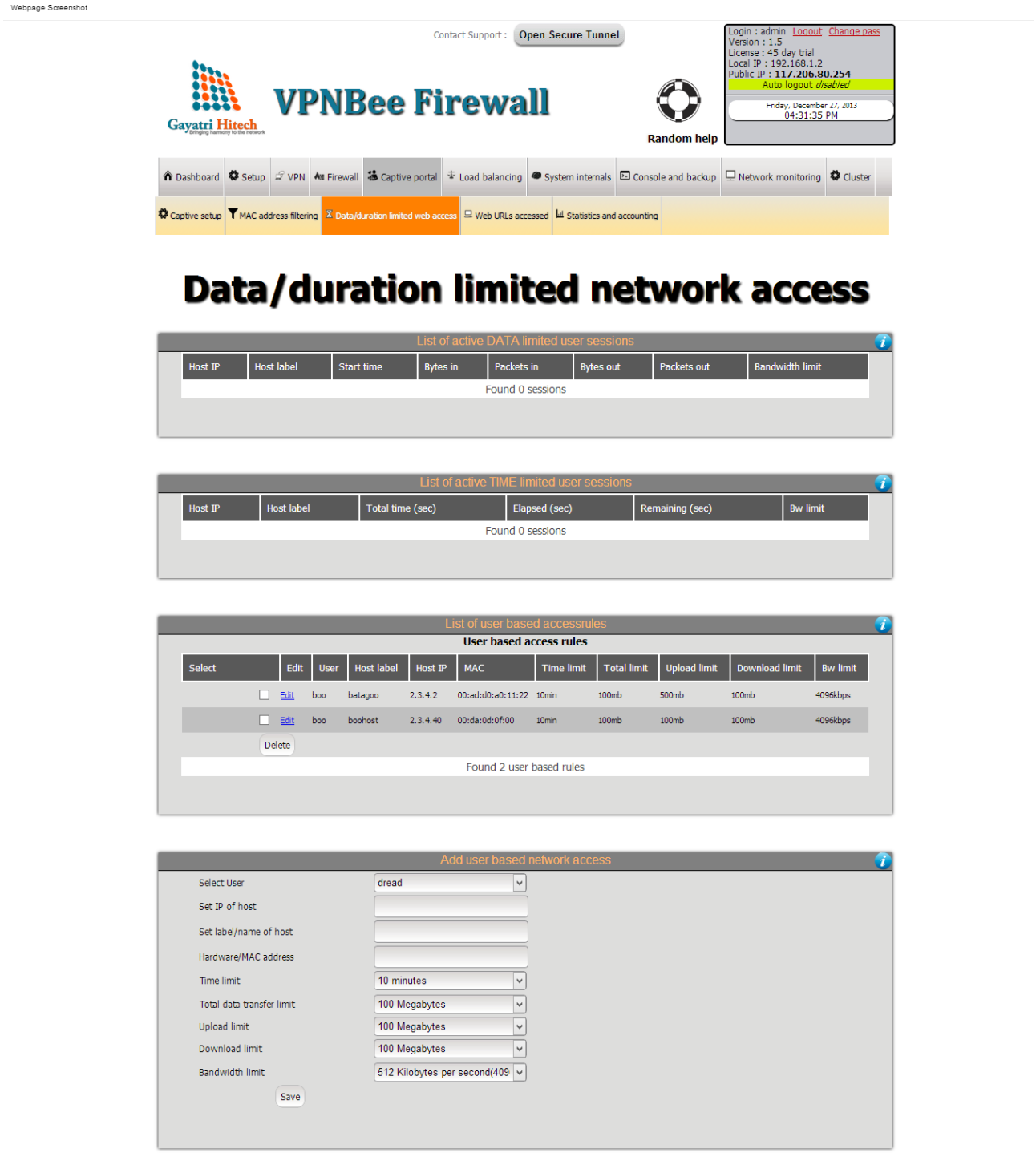
Save

You can then view the **MAC address filtering** menu. This need not be used only for captive portal but also used outside of it. You can list the MAC addresses that you want to allow access.



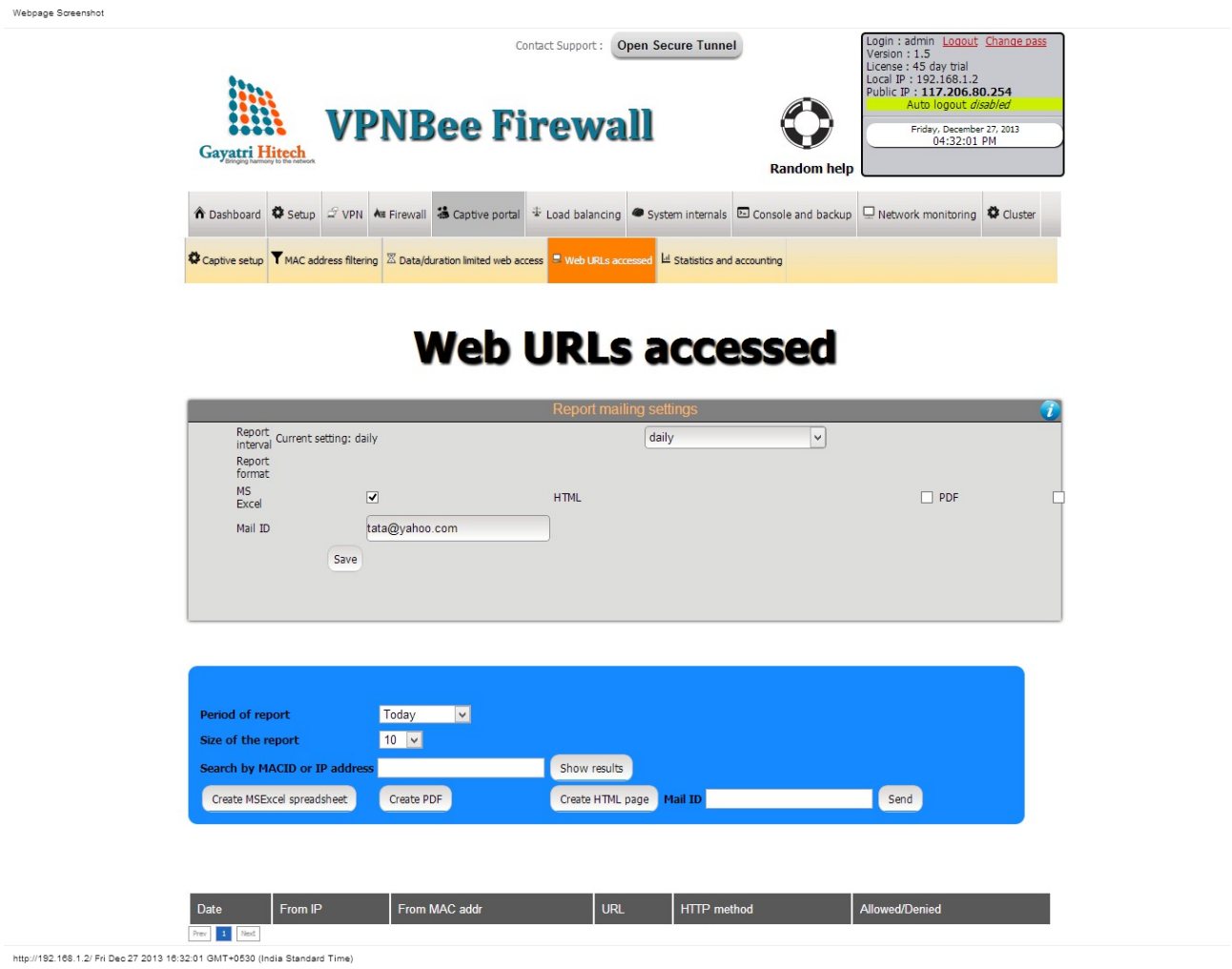
Then you have the important **Data/duration limited web access** screen. After setting up users using the **Captive setup** you have to assign the upload and download limits and time limits using this screen.

You can also view the currently active time limited and data limited sessions. Each of these sessions are logged into a backend database for billing purposes.



Then you have the **Web URLs accessed** menu. Each of the hosts accessing the web from the captive portal as setup the URLs they access, the MAC and IP address, the time of access and the allow/deny status are logged here.

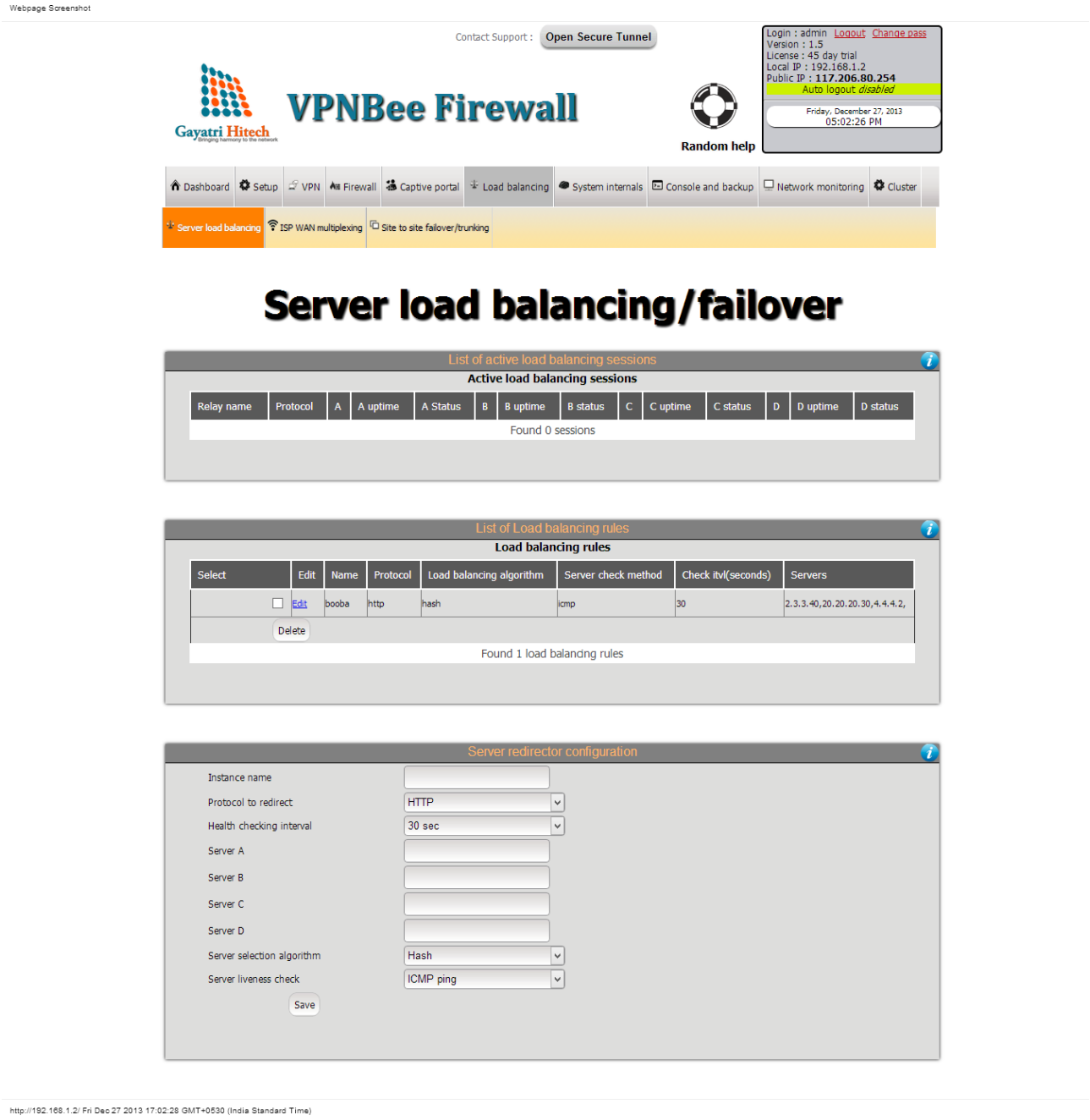
You can optionally have this info mailed as well as export this data in **PDF, HTML or MS Excel** formats.



Then finally you have the **Statistics and accounting** menu. Using this you can calculate the rates you wish to charge each captive user.

After captive portal we can look at the next data center/server side feature of VPNBee, the **Load balancing -> Server load balancing** menu. This page does what is called a service redirector activity in which each protocol that lands is redirected to a group of hosts based on an algorithm like random, round robin, source hash etc.

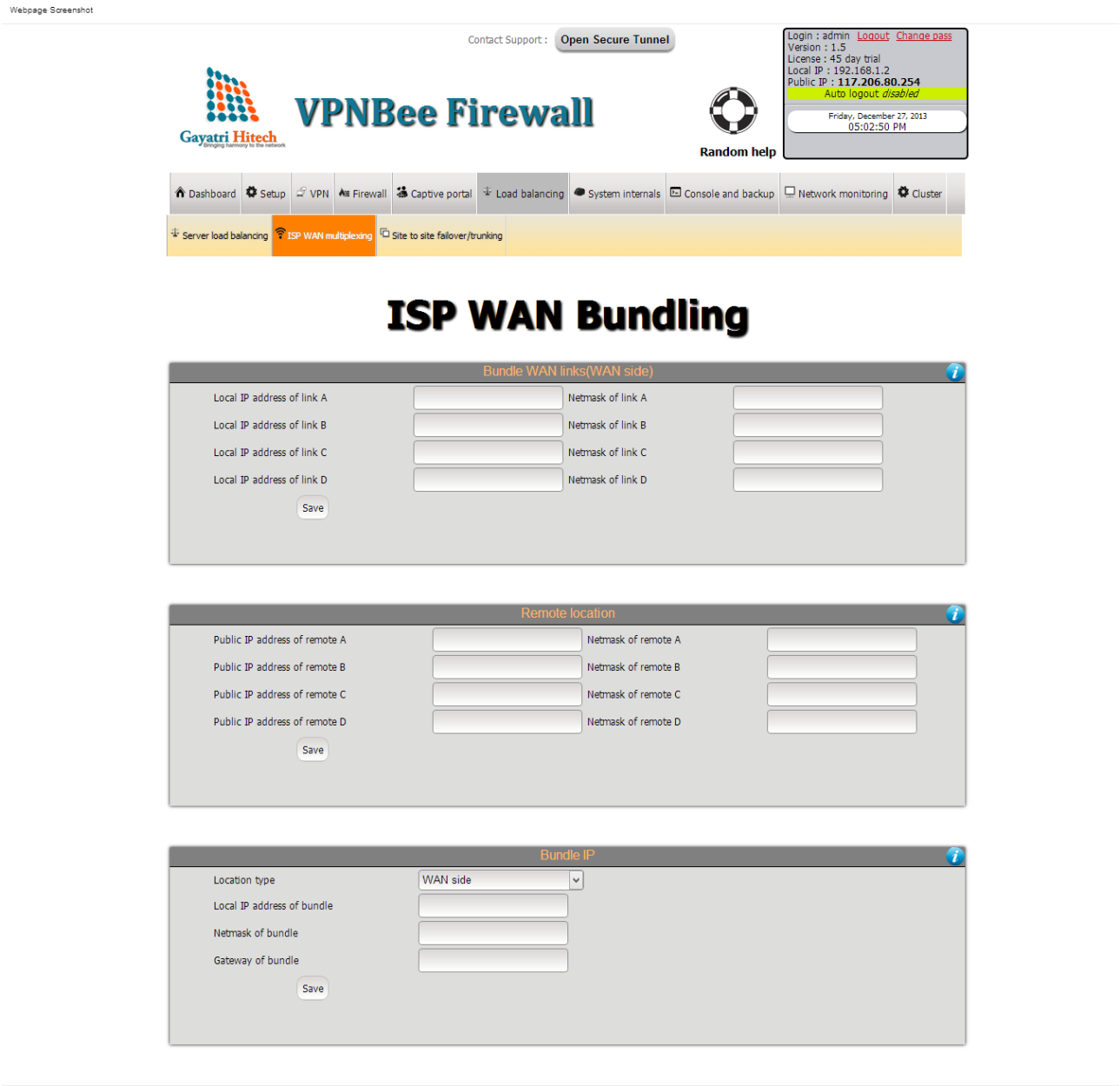
You can also view the list of server load balanced hosts here. Health checks and SSL acceleration can also be performed.



Then you can click at **ISP WAN multiplexing** should you be interested in bundling various ISP links together.

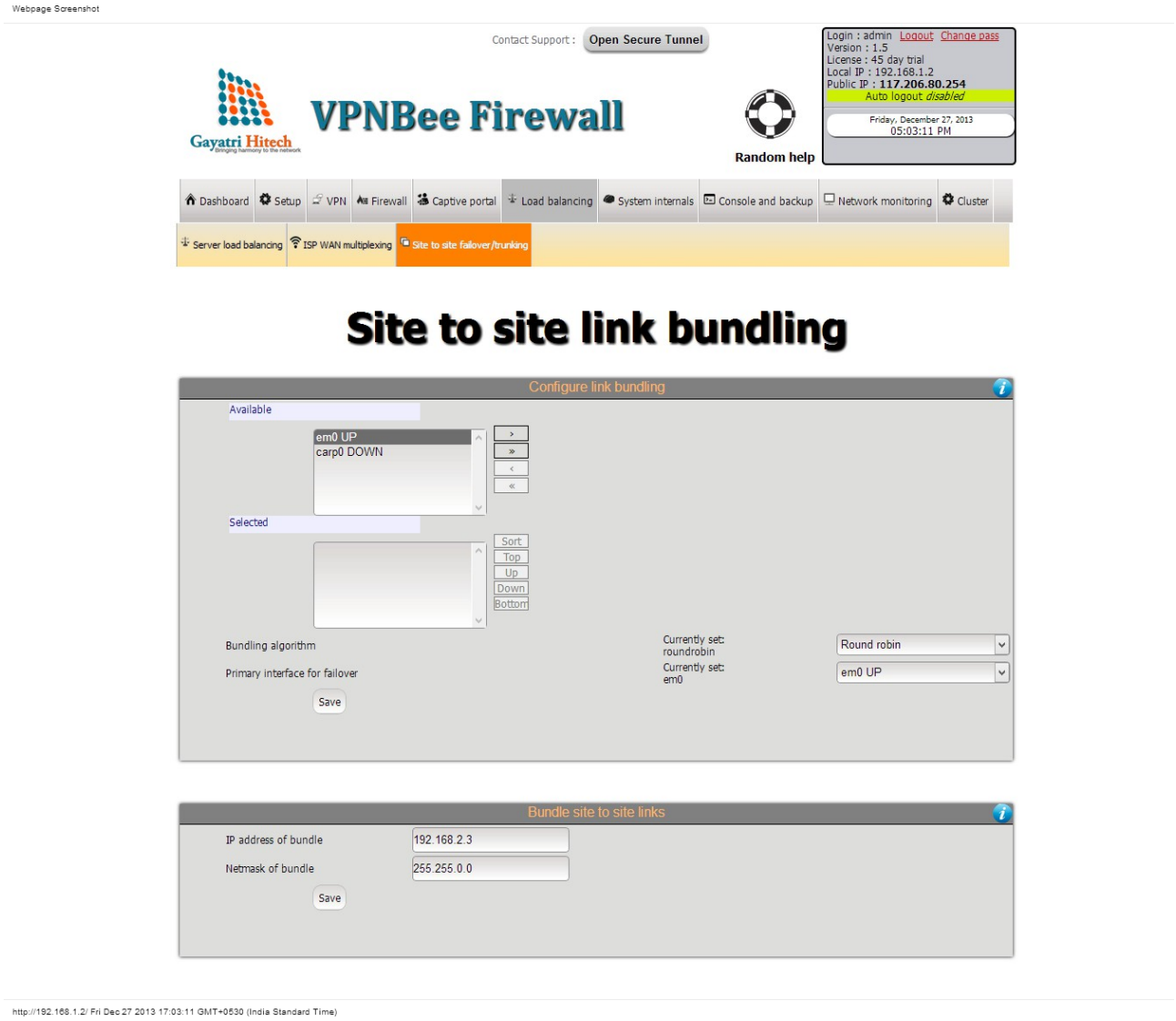
In order to accomplish true link bundling you will have to setup VPNs with a public server with high bandwidth and all traffic outside of your network will actually leave out through the public server which is typically a VPS node.

You can run VPNBee at both ends and setup the link bundles.



Finally you the **Site to site failover/trunking** menu item. Using this you can setup a bundle of identical termination points and assign the same IP address but depending on the priority and algorithm only one link will be active at a time.

This is useful for branch office deployments when a copper or optic link is preferred over a wireless link that is less reliable and less speedy.



Then you have the **System internals -> Traffic meter**. This is the traffic meter screen which shows the incoming traffic patterns live as well as the the bar graph of the traffic patterns over the daily weekly and monthly time periods.

Contact Support : Open Secure Tunnel

Login : admin Logout Change pass
Version : 1.5
License : 45 day trial
Local IP : 192.168.1.2
Public IP : **117.206.80.254**
Auto logout *disabled*
Friday, December 27, 2013
05:08:30 PM

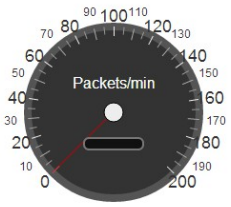
Gayatri Hitech
bringing harmony to the network

VPNBee Firewall

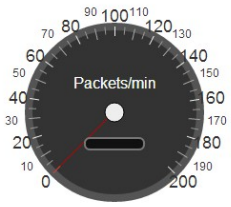
Random help

Dashboard | Setup | VPN | Firewall | Captive portal | Load balancing | System internals | Console and backup | Network monitoring | Cluster

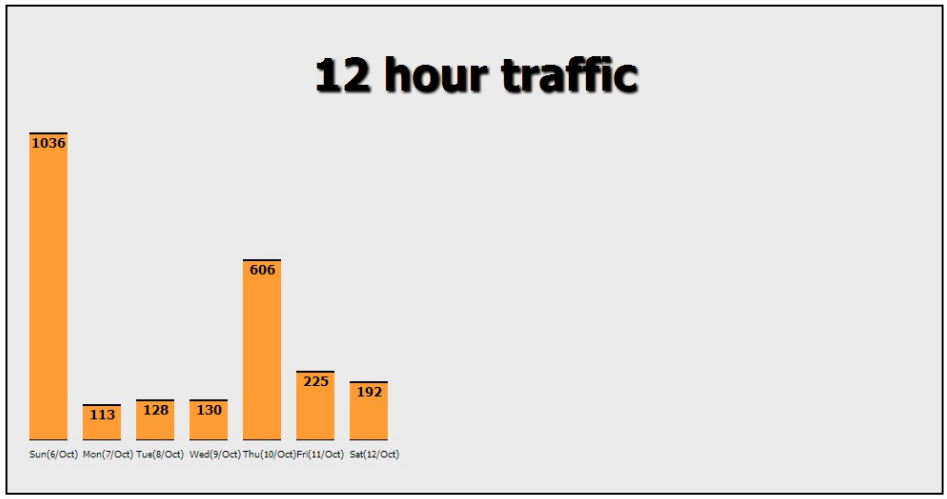
Traffic meter | System info | Live Web Log View | Graphs | Reporting | Edit Logs | System logs

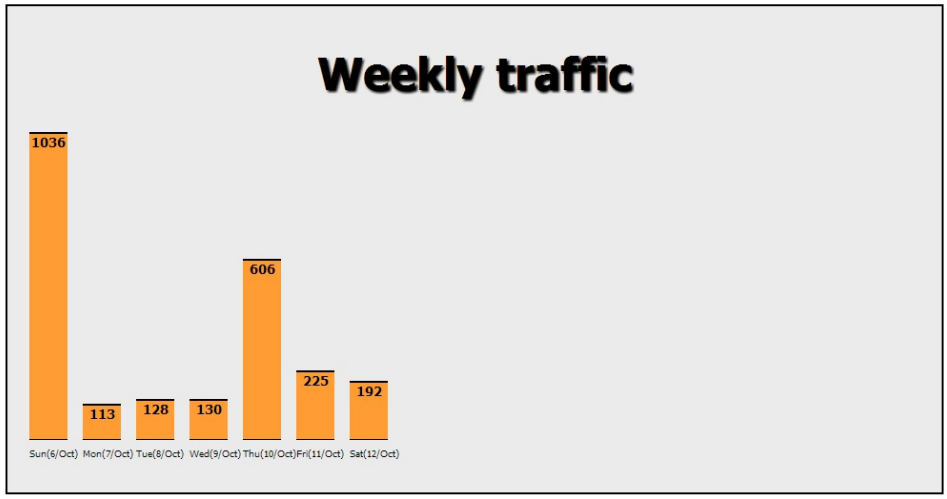


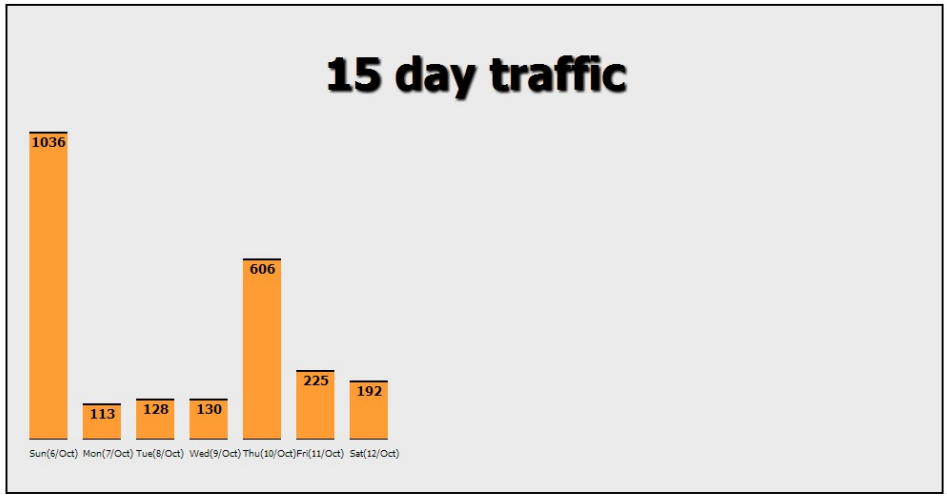
IN packets



OUT packets







Then you have the longest screen in VPNBee **System Info**.

You have a cornucopia of tools as well as diagnostic info in the screen.

Contact Support : Open Secure Tunnel

Gayatri Hitech

VPNBee Firewall

Random help

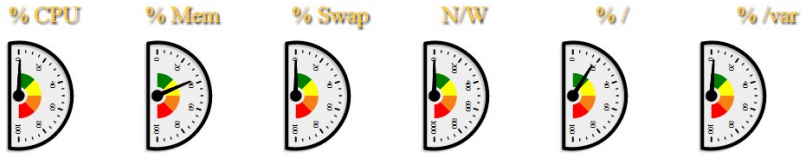
Login : admin Logout Change pass
Version : 1.5
License : 45 day trial
Local IP : 192.168.1.2
Public IP : **117.206.80.254**
Auto logout *disabled*

Friday, December 27, 2013
05:08:58 PM

Dashboard | Setup | VPN | Firewall | Captive portal | Load balancing | System internals | Console and backup | Network monitoring | Cluster

Traffic meter | System info | Live Web Log View | Graphs | Reporting | Edit Logs | System logs

System running info



Live graph of system health

Show Realtime graph

System Info

TR>

Processor	Intel(R) Core(TM) i3-3120M CPU @ 2.50GHz
Memory	39%
CPU Usage	1%
Disk usage on / partition	18%
Disk usage on /var partition	2%
Load	1.13,1.13,1.13
Number of Processes	53
Uptime	day 6:22 0 hours

Daemons

ISAKMPD IKE Daemon DOWN START RESTART

System Internals

Process List Show

Network connections Show

Routing Table Show

System Health Report

System uptime day 6:22 0 hours
Number of Processes 53
System vital parameters check Health check

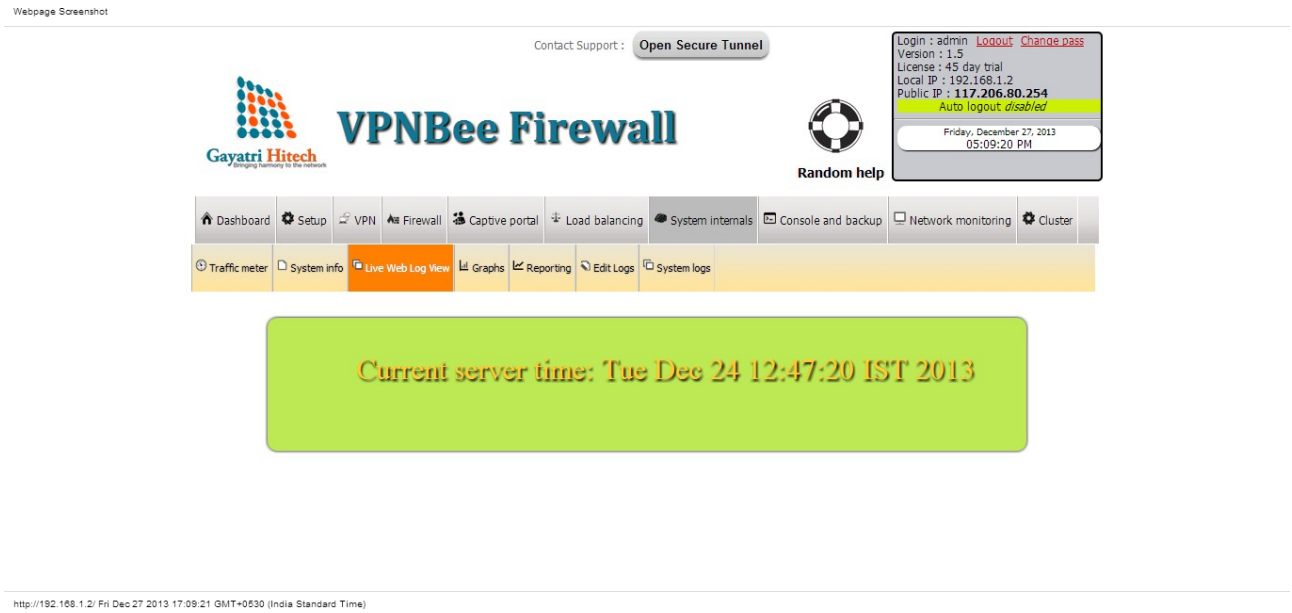
Diagnostic tools

Ping a host by DNS/IP Ping

Traceroute a host by DNS/IP Trace

Diagnostic results

Then you have the **Live web log view** screen which shows the live view of the web access done thro' VPNBee.



Then you have the **Graphs** view which shows the various firewall parameters in a time series display by week, month and year.

Contact Support : Open Secure Tunnel

Gayatri Hitech

VPNBee Firewall

Random help

Login : admin Logout Change pass
Version : 1.5
License : 45 day trial
Local IP : 192.168.1.2
Public IP : 117.206.80.254
Auto logout disabled
Friday, December 27, 2013
05:09:45 PM

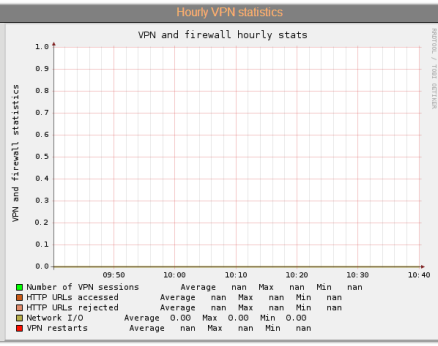
Graphical representation of VPN traffic

VPNBee
VPN graphs

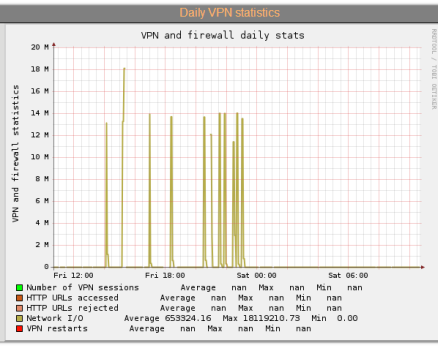
Hourly traffic

Weekly traffic

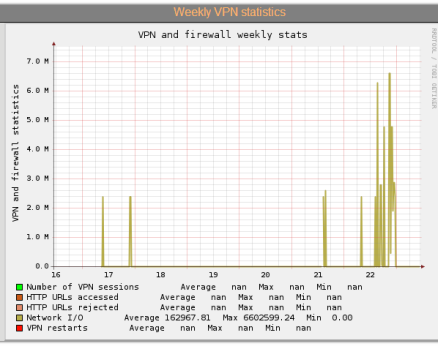
Hourly VPN statistics


VPN and firewall hourly stats
VPN and firewall statistics
09:50
10:00
10:10
10:20
10:30
10:40
Number of VPN sessions Average nan Max nan Min nan
HTTP URLs accessed Average nan Max nan Min nan
HTTP URLs rejected Average nan Max nan Min nan
Network I/O Average 0.00 Max 0.00 Min 0.00
VPN restarts Average nan Max nan Min nan

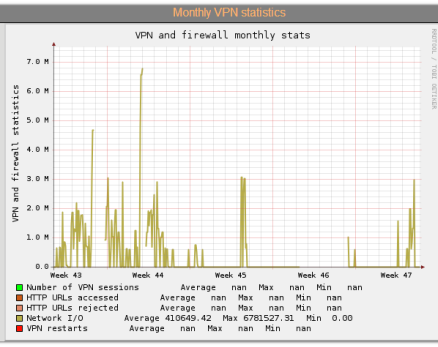
Daily VPN statistics


VPN and firewall daily stats
VPN and firewall statistics
Fri 12:00
Fri 18:00
Sat 00:00
Sat 06:00
Number of VPN sessions Average nan Max nan Min nan
HTTP URLs accessed Average nan Max nan Min nan
HTTP URLs rejected Average nan Max nan Min nan
Network I/O Average 653324.16 Max 18119210.73 Min 0.00
VPN restarts Average nan Max nan Min nan

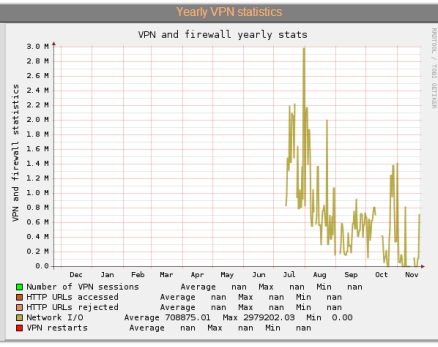
Weekly VPN statistics


VPN and firewall weekly stats
VPN and firewall statistics
16
17
18
19
20
21
22
Number of VPN sessions Average nan Max nan Min nan
HTTP URLs accessed Average nan Max nan Min nan
HTTP URLs rejected Average nan Max nan Min nan
Network I/O Average 162967.81 Max 6602599.24 Min 0.00
VPN restarts Average nan Max nan Min nan

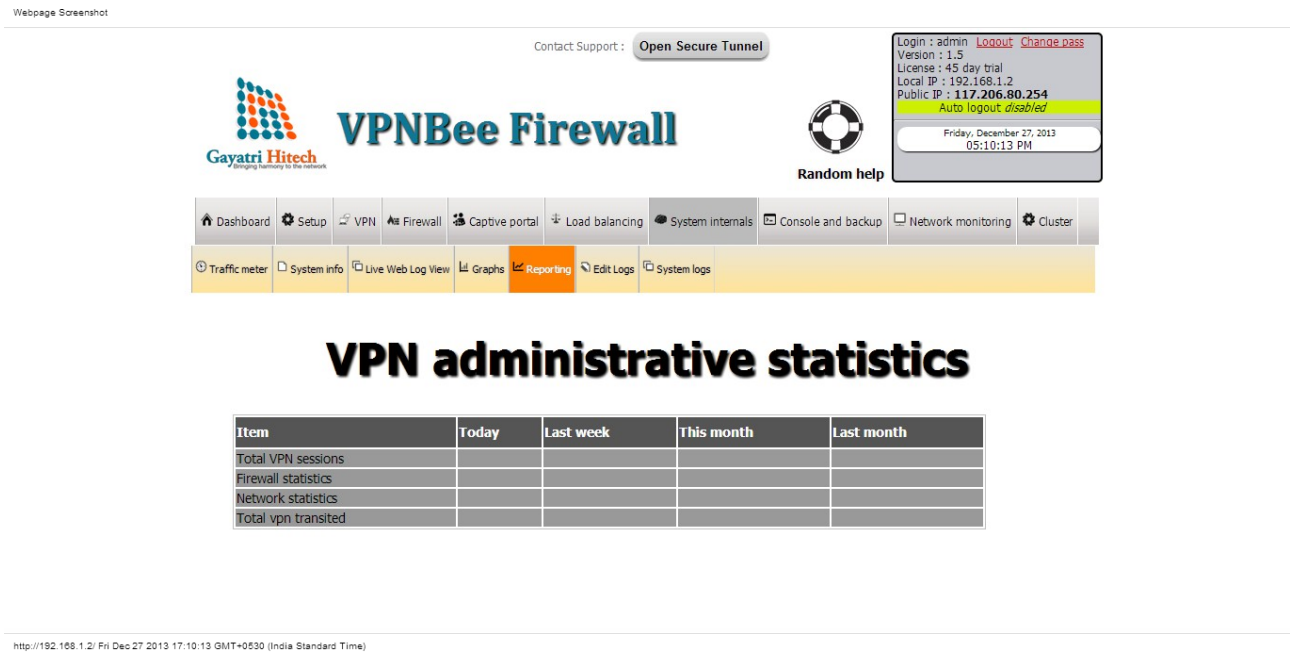
Monthly VPN statistics


VPN and firewall monthly stats
VPN and firewall statistics
Week 43
Week 44
Week 45
Week 46
Week 47
Number of VPN sessions Average nan Max nan Min nan
HTTP URLs accessed Average nan Max nan Min nan
HTTP URLs rejected Average nan Max nan Min nan
Network I/O Average 410649.42 Max 6781527.31 Min 0.00
VPN restarts Average nan Max nan Min nan

Yearly VPN statistics

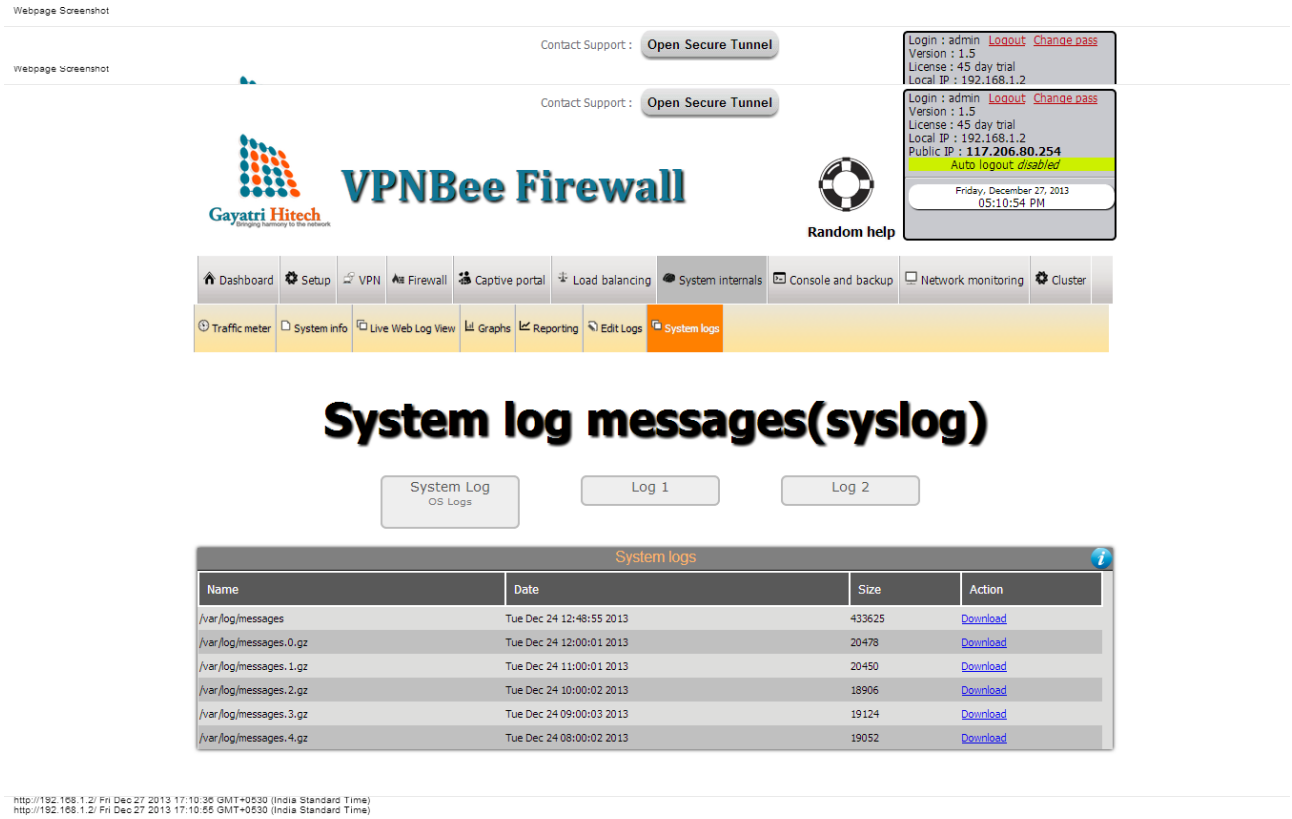


Then you have the **Reporting, Edit logs** and **Syslog** screens.



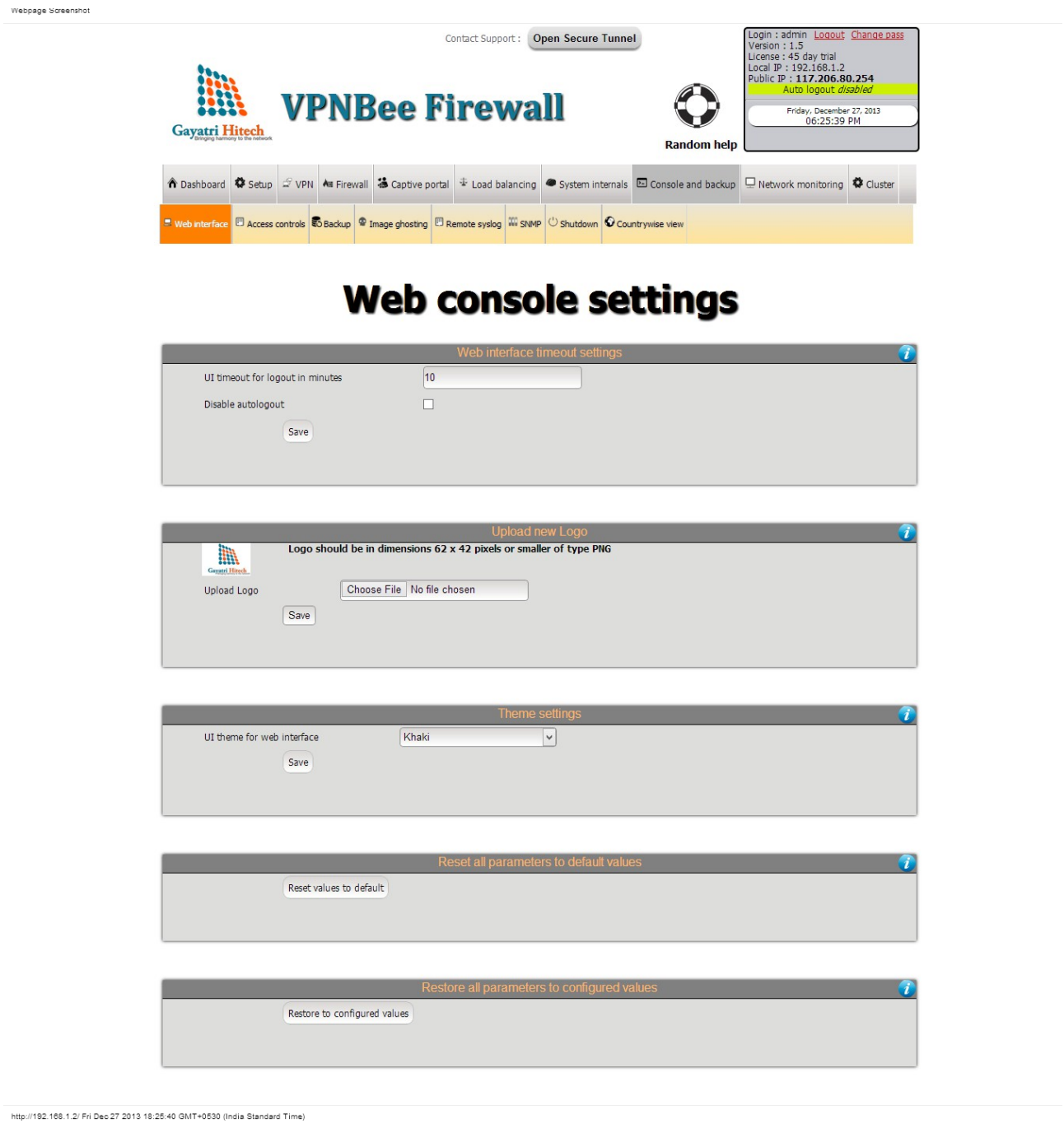
The **Edit logs** and **Syslog** screens show the web console edit logs as well as the system logs which help you view the log files for offline viewing.

The reporting screen above shows the most vital statistics of VPNBee in a very easy to view fashion.

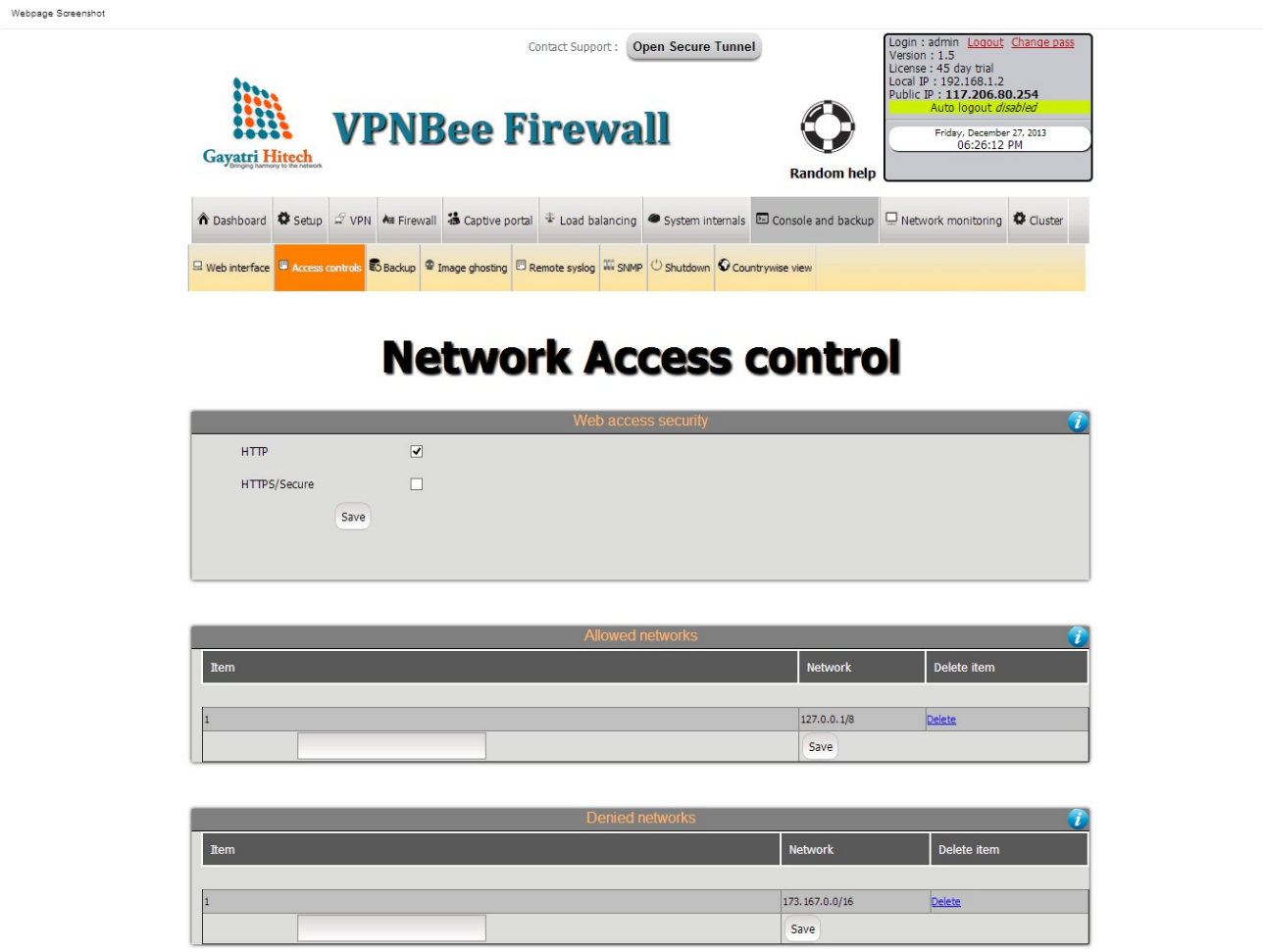


The next screen to view is the **Console and backup -> Web interface**. You can

configure the themes/skins and upload the logo of VPNBee using this interface.



Then you can click at the **Access controls** menu. You can easily figure out what the screen does.



The **Backup** screen helps you take backup and restore the backend database of VPNBee either using rsnapshot or either manually.

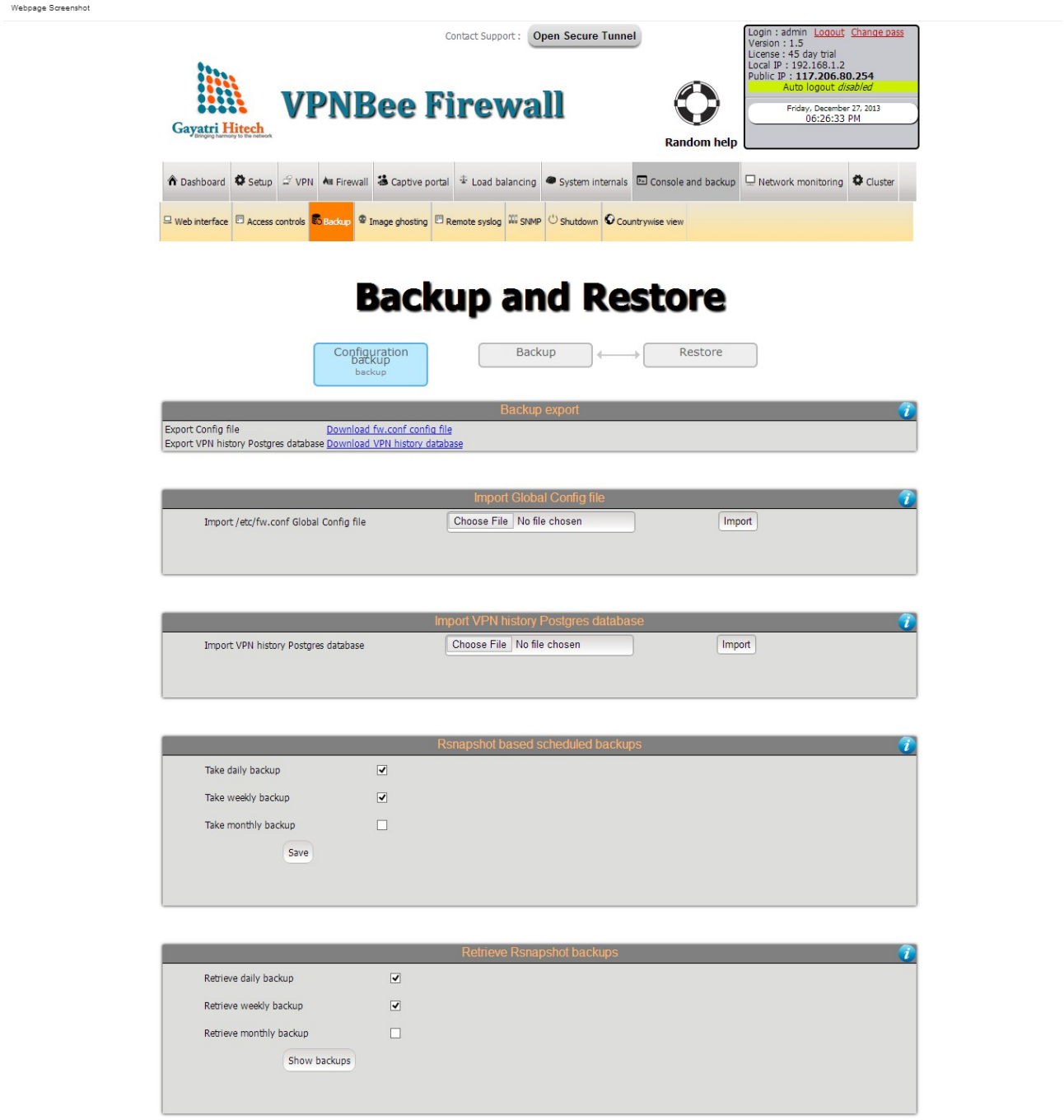
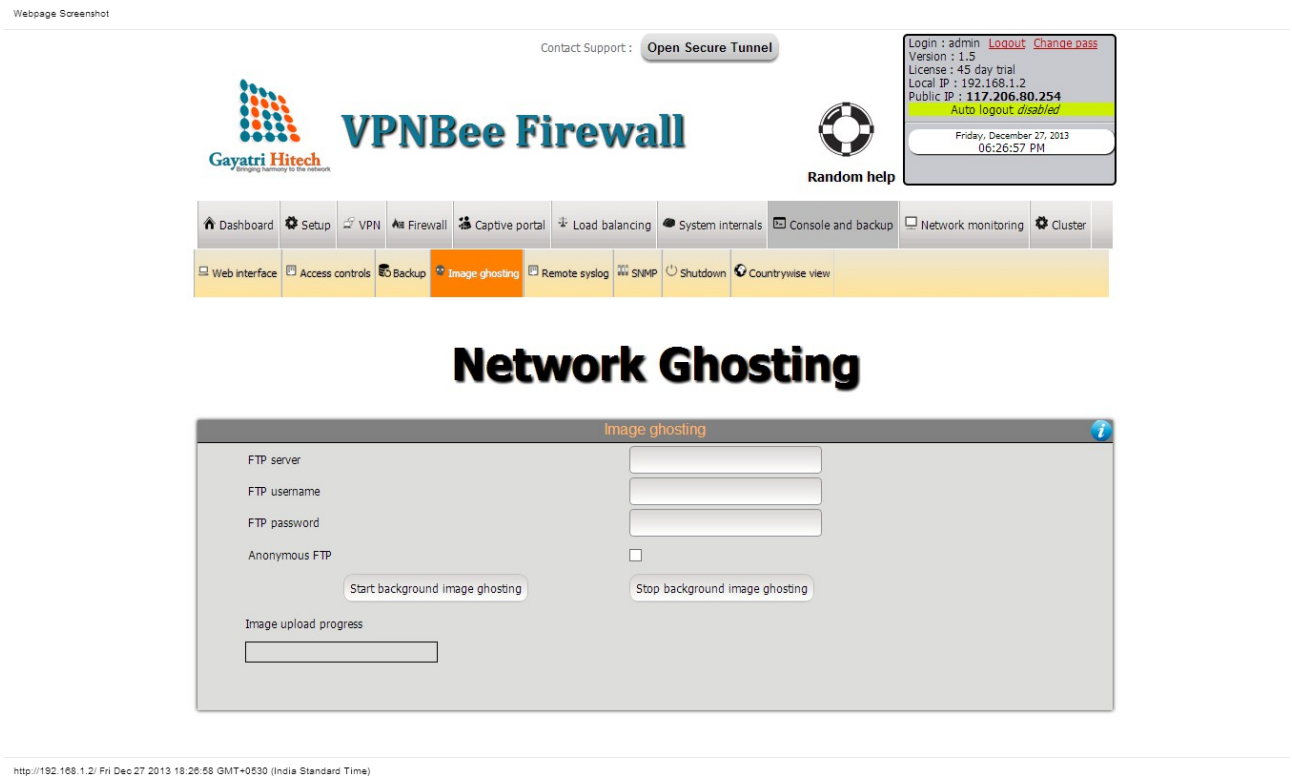
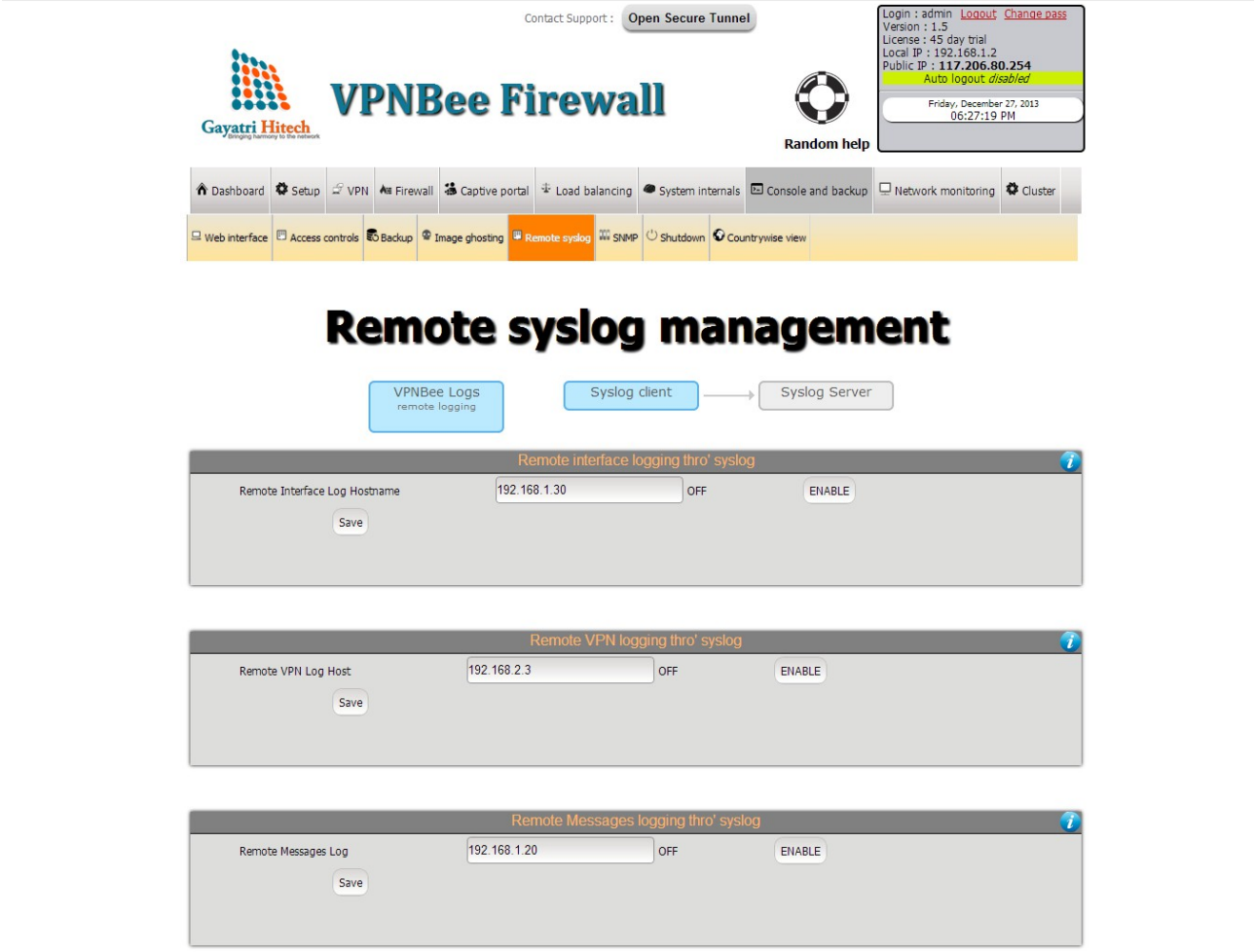


Image ghosting is the screen using which you can upload the bit by bit ghosted image of VPNBee to an FTP server.



Then you have the **Remote syslog** menu in which we can setup a log server in the local LAN which can gather the logs from VPNBee.

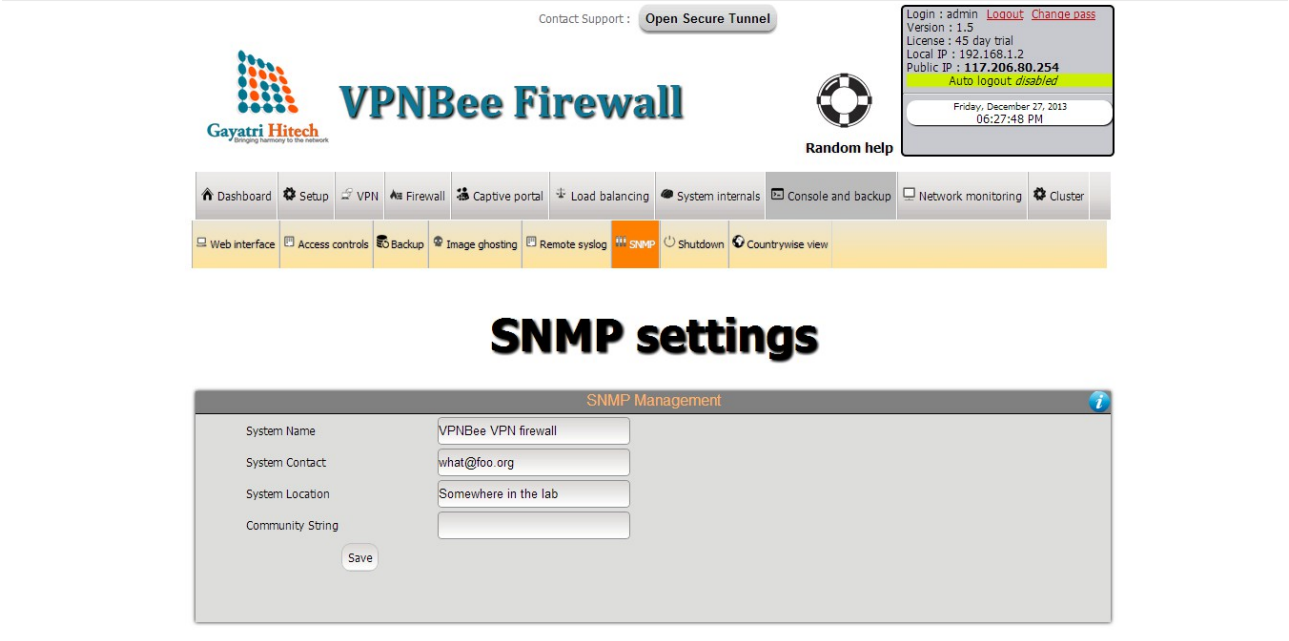
Webpage Screenshot



http://192.168.1.2/ Fri Dec 27 2013 18:27:20 GMT+0530 (India Standard Time)

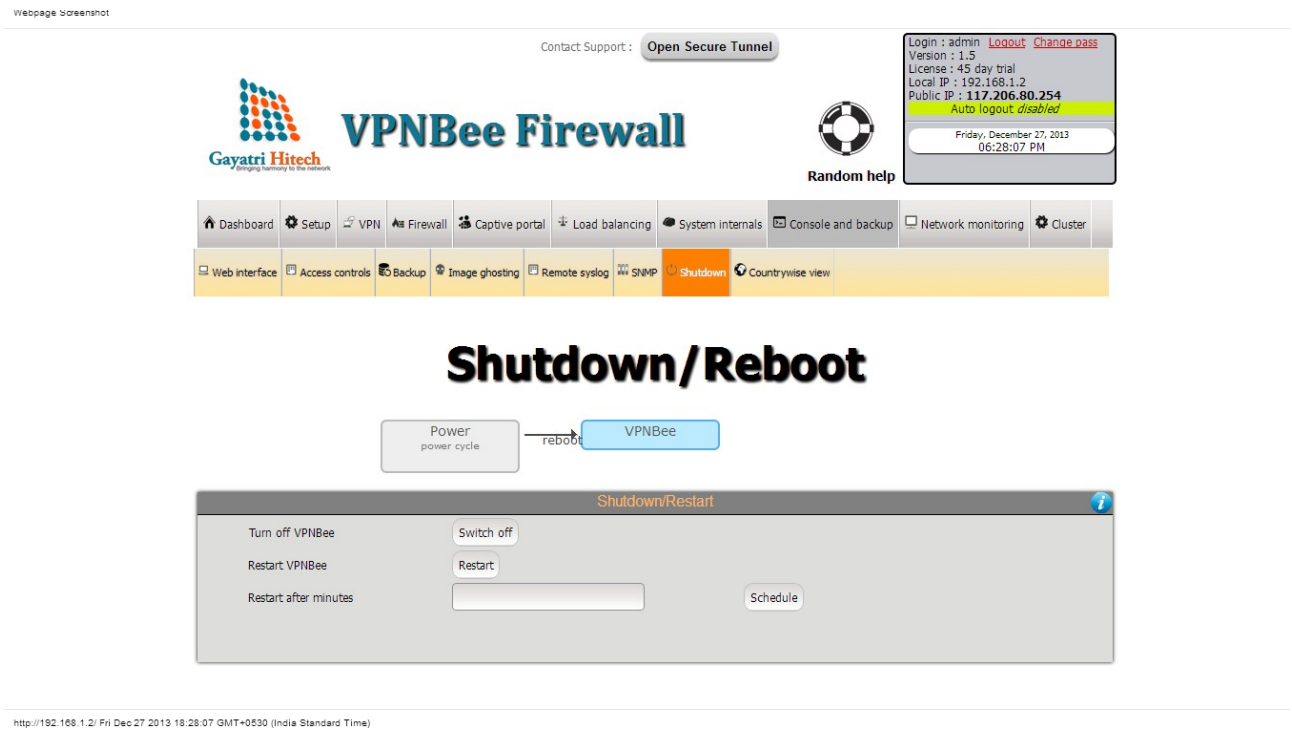
The **SNMP** settings menu helps you setup the SNMP system name, system contact e-mail address, system location etc.

Webpage Screenshot



http://192.168.1.2/ Fri Dec 27 2013 18:27:48 GMT+0530 (India Standard Time)

The **Shutdown** menu helps you shutdown or reboot VPNBee for maintenance.



The **Countrywise view** screen helps you show the countries from which the hosts connecting to the network protected by VPNBee in a **choropleth** view.

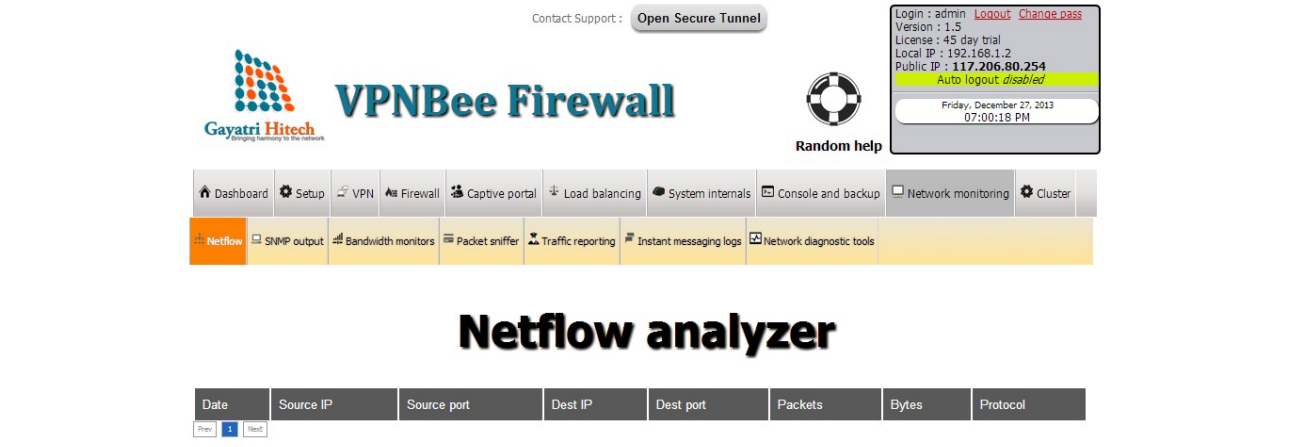
You can easily spot the countries sending the highest number of packets in a reverse sorted top 50 countries.

Webpage Screenshot

http://192.168.1.2/ Fri Dec 27 2013 18:28:29 GMT+0530 (India Standard Time)

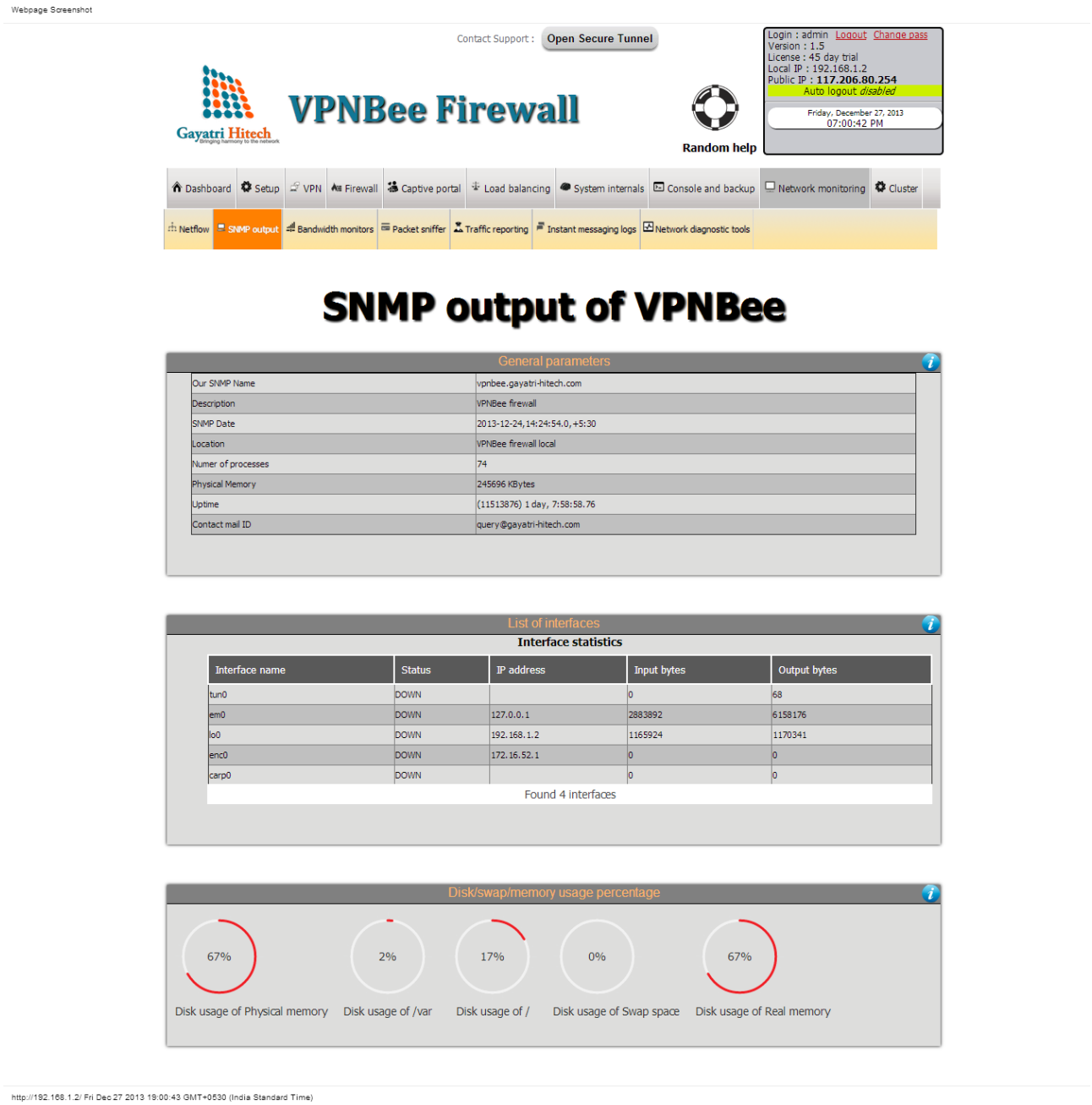
Then you have the **Network monitoring -> Netflow** menu. This page shows the traffic flows in the network using Netflow v9. Netflow collects enormous amounts of data in a busy network and so VPNBee stores only the latest information it can keep.

Webpage Screenshot



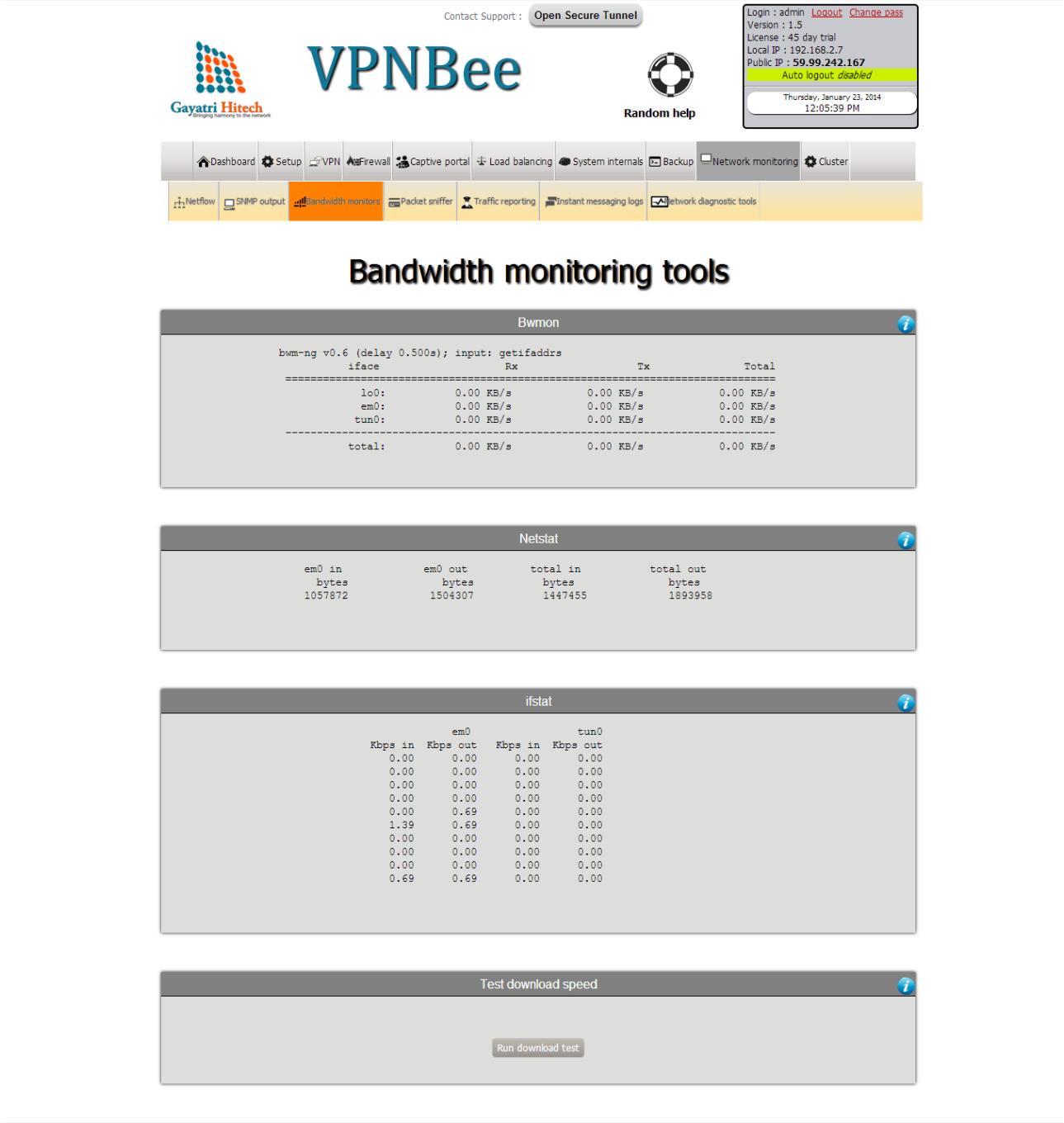
http://192.168.1.2/ Fri Dec 27 2013 19:00:19 GMT+0530 (India Standard Time)

The **SNMP Output** screen shows the SNMP parameters dished out by VPNBee on the network. This can be a very detailed and useful dump of the current disk use, network use and other vital parameters' latest values.



Then you could look at **Bandwidth monitors** for figuring out the latest bandwidth usage patterns of VPNBee.

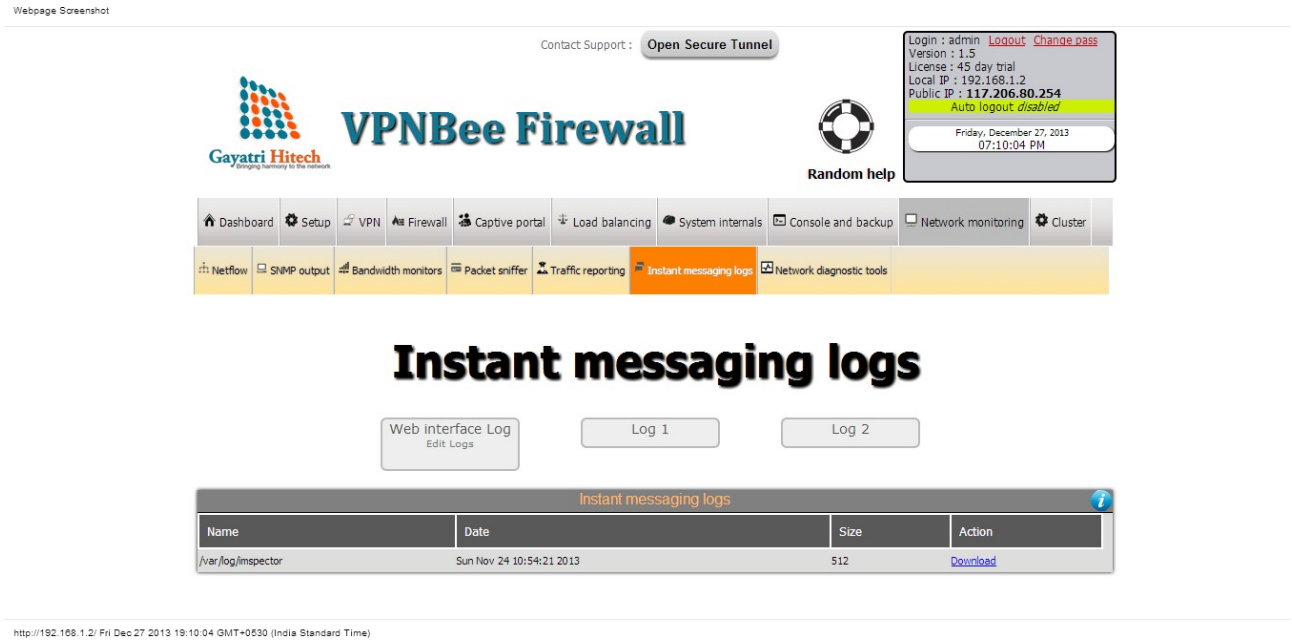
Webpage Screenshot



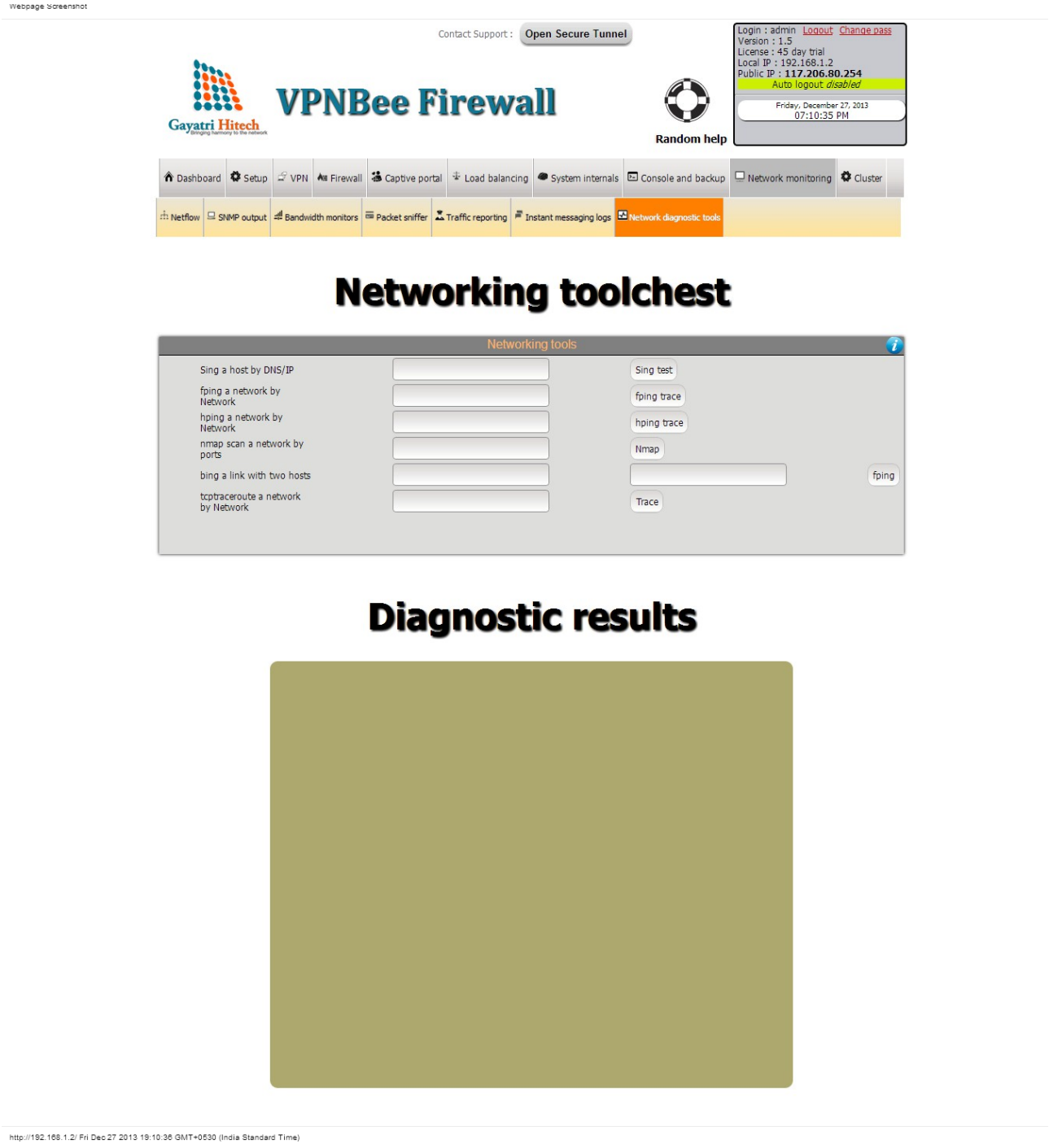
Then you have a **Packet sniffer** menu which shows the packet sniffer output which has a tcpdump filter using which you can look for packets matching certain filter patterns.

You also have a **Traffic reporting** screen which shows you the network traffic as saved in the internal database of VPNBee which can be exported in **MS Excel, PDF or HTML formats.**

Then you have the **Instant messaging log**s which shows the log of the various unencrypted chat protocols in use in the local network.



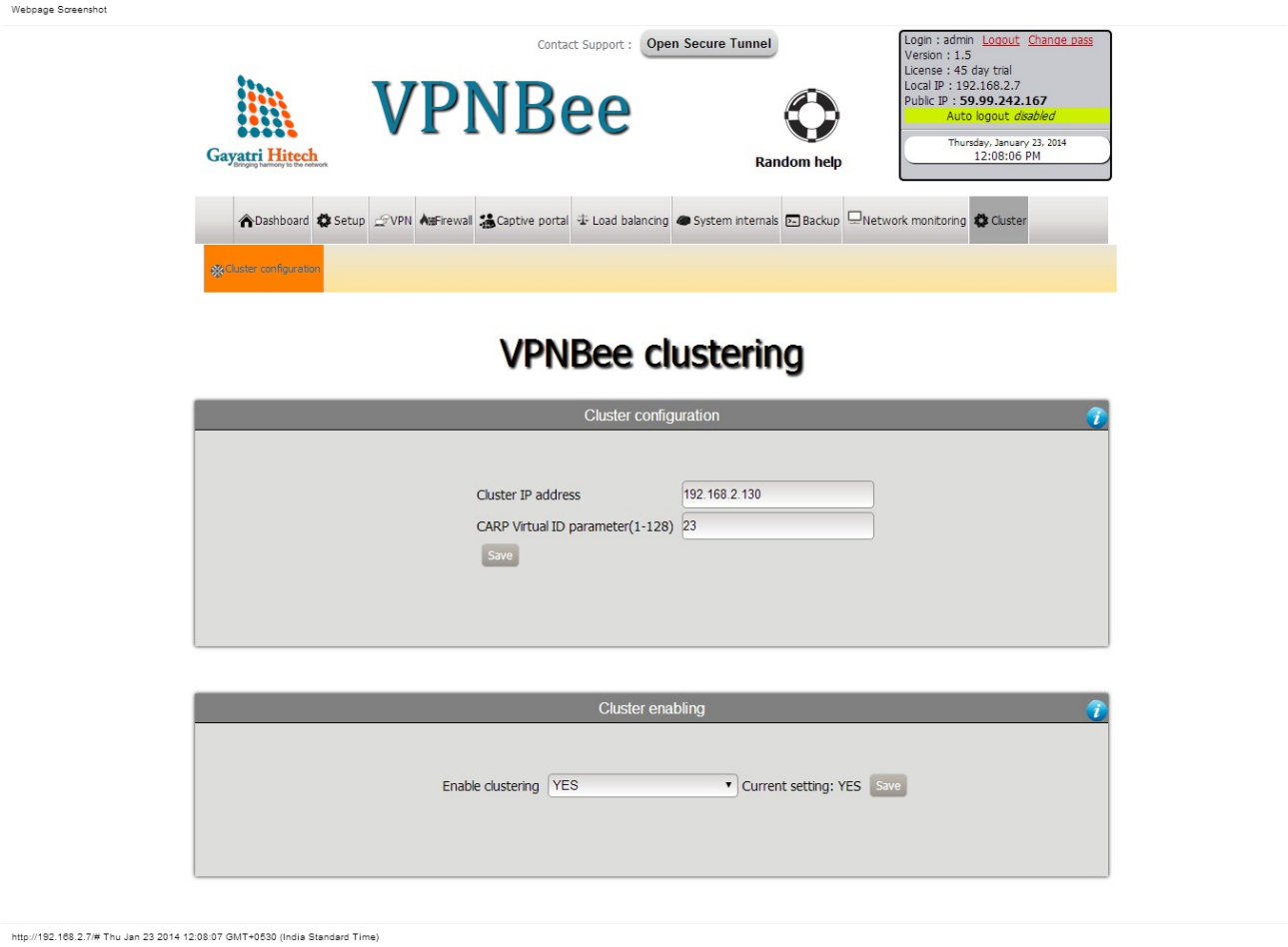
You then have the **Network diagnostic tools** menu which gives you a cornucopia of network snooping and diagnostic tools of value to a UNIX administrator available in an easy to use web interface.



Finally VPNBee is cluster ready and you can setup clustering very easily using the **Clustering -> Cluster** menu item.

VPNBee employs a protocol called CARP , Common Address Redundancy protocol which is a very simple way of obtaining 100% uptime guarantee by using a cluster IP address which is assigned to all the nodes participating in the VPNBee cluster.

Only one of the nodes will be the master and all others will be slaves in this cluster.



The VHID parameter can be left unchanged if you have only one cluster in your network.

VPNBee is a fairly complex product with many functionalities but it is easy to adminster and maintain as it has many diagnostic tools to unearth what is going on underneath.